PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-273856
(43)Date of publication of application : 26.09.2003

(51)Int.Cl. H04L 9/08
G09C 1/00
H04J 11/00
H04J 13/00
H04Q 7/38

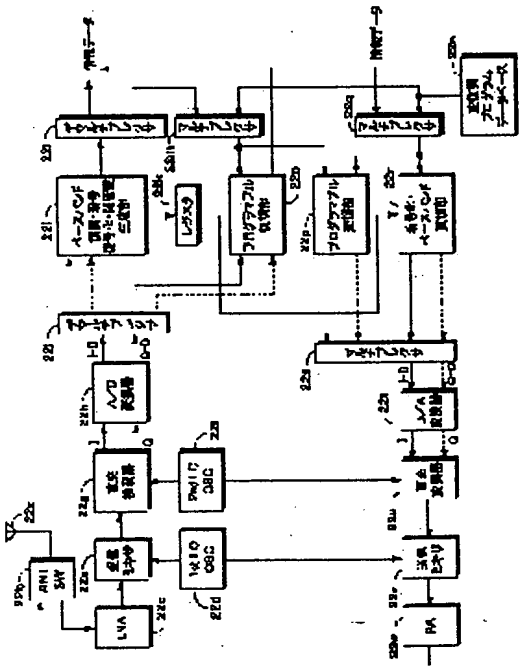
(21)Application number : 2002-069516
(22)Date of filing : 14.03.2002

(71)Applicant : COMMUNICATION RESEARCH LABORATORY
TEKTRONIX JAPAN LTD

(72)Inventor : HONDA MAKOTO
HARADA HIROSHI
FUJISE MASAYUKI

(54) COMMUNICATION APPARATUS AND COMMUNICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide radio transmission for information or program data with higher secrecy, without the need of private key transmission.
SOLUTION: A received digital baseband signal is supplied to a baseband demodulation/cipher decryption/private key generation unit 22j or a programmable demodulation unit 22o. At the baseband demodulation/cipher decryption/private key generation unit 22j, a private key for decryption of a demodulation/error correction codes and for encryption and cipher decryption is generated, and cipher decryption is conducted to output the decrypted cipher as information data or a modulation/demodulation program. According to the modulation/demodulation program, a modulation/demodulation device of the desired specification is configured. Transmission information data or program is processed for encryption, error correction encoding, and digital modulation by the private key at an encryption/baseband modulation unit 22r. The encryption/baseband modulation unit 22r outputs baseband digital data.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－273856
（P2003－273856A）
(43)公開日　平成15年９月26日(2003.9.26)

(51)Int.Cl.'		識別記号	Ｆ Ｉ		テーマコード'(参考)
Ｈ０４Ｌ	9/08		Ｇ０９Ｃ	1/00	６５０Ｂ　５Ｊ１０４
Ｇ０９Ｃ	1/00	６５０	Ｈ０４Ｊ	11/00	５Ｋ０２２
Ｈ０４Ｊ	11/00		Ｈ０４Ｌ	9/00	６０１Ａ　５Ｋ０６７
	13/00		Ｈ０４Ｂ	7/26	１０９Ｒ
Ｈ０４Ｑ	7/38		Ｈ０４Ｌ	9/00	６０１Ｅ

審査請求　未請求　請求項の数16　ＯＬ　（全 23 頁）　最終頁に続く

(21)出願番号　特願2002－69516(P2002－69516)

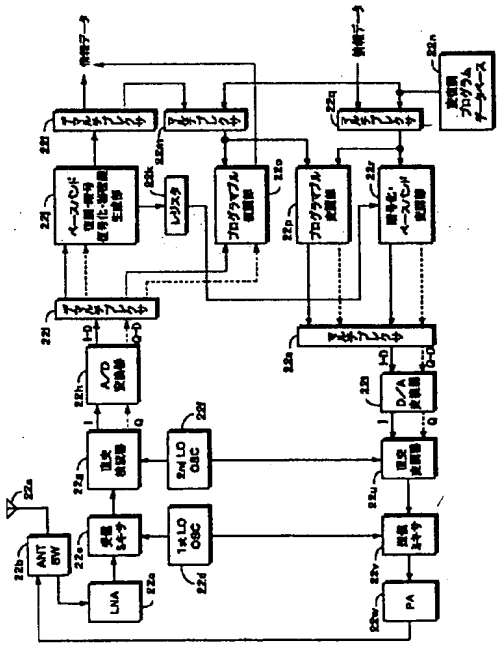
(22)出願日　平成14年３月14日(2002.3.14)

(71)出願人　301022471
独立行政法人通信総合研究所
東京都小金井市貫井北町４－２－１
(71)出願人　000108409
日本テクトロニクス株式会社
東京都品川区北品川５丁目９番31号
(72)発明者　本多　真
東京都品川区北品川５丁目９番31号　ソニー・テクトロニクス株式会社内
(74)代理人　100082762
弁理士　杉浦　正知

最終頁に続く

(54)【発明の名称】　通信装置および通信方法

(57)【要約】
【課題】　秘密鍵を伝送する必要がなく、高い機密性で情報またはプログラムデータを無線伝送する。
【解決手段】　受信ディジタルベースバンド信号がベースバンド復調・暗号復号化・秘密鍵生成部２２ｊまたはプログラマブル復調部２２ｏに供給される。ベースバンド復調・暗号復号化・秘密鍵生成部２２ｊにおいては、復調・誤り訂正符号の復号化、さらに、暗号化と暗号復号化のための秘密鍵が生成され、暗号の復号化が行われて情報データまたは変復調プログラムとして出力される。変復調プログラムにしたがって所望の仕様の変復調器が構成される。送信情報データまたはプログラムが秘密鍵によって暗号化・ベースバンド変調部２２ｒにおいて暗号化、誤り訂正符号化、ディジタル変調の処理を受ける。暗号化・ベースバンド変調部２２ｒは、ベースバンドディジタルデータを出力する。



【特許請求の範囲】
【請求項１】　略同一のキャリア周波数を時分割に使用して他の通信装置との間で送信および受信を交互に行なう無線通信システムにおける通信装置において、
既知の信号に基づいて、上記他の通信装置との間の伝搬路の遅延プロファイルを推定する手段と、
推定した上記遅延プロファイルの複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成する手段と、
上記秘密鍵を用いて情報データを暗号化して送信し、または上記秘密鍵で暗号化された情報データを受信して復号化を行なう手段とを有する通信装置。
【請求項２】　略同一のキャリア周波数を時分割に使用して他の通信装置との間で送信および受信を交互に行なう無線通信システムにおける通信装置において、
既知の信号に基づいて、上記他の通信装置との間の伝搬路の周波数特性を推定する手段と、
推定した上記周波数特性の複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成する手段と、
上記秘密鍵を用いて情報データを暗号化して送信し、または上記秘密鍵で暗号化された情報データを受信して復号化を行なう手段とを有する通信装置。
【請求項３】　略同一のキャリア周波数を時分割に使用して他の通信装置との間で送信および受信を交互に行なう無線通信システムにおける通信装置であって、
ハードウェアの一部または全部がプログラム可能な論理回路で構成され、論理回路に対するプログラムデータによって、所望の無線通信方式を実現するようにした通信装置において、
既知の信号に基づいて、上記他の通信装置との間の伝搬路の遅延プロファイルを推定する手段と、
推定した上記遅延プロファイルの複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成する手段と、
上記秘密鍵を用いてプログラムデータを暗号化して送信し、または上記秘密鍵で暗号化されたプログラムデータを受信して復号化を行なう手段とを有する通信装置。
【請求項４】　略同一のキャリア周波数を時分割に使用して他の通信装置との間で送信および受信を交互に行なう無線通信システムにおける通信装置であって、
ハードウェアの一部または全部がプログラム可能な論理回路で構成され、論理回路に対するプログラムデータによって、所望の無線通信方式を実現するようにした通信装置において、
既知の信号に基づいて、上記他の通信装置との間の伝搬路の周波数特性を推定する手段と、
推定した上記周波数特性の複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成する手段と、
上記秘密鍵を用いてプログラムデータを暗号化して送信し、または上記秘密鍵で暗号化されたプログラムデータを受信して復号化を行なう手段とを有する通信装置。
【請求項５】　請求項１、２、３または４において、
他の通信装置から受信した受信信号中の上記既知の信号に基づいて、上記伝搬路の遅延プロファイルまたは上記周波数特性を推定する通信装置。
【請求項６】　請求項１、２、３または４において、
内部に既知の信号を使用して伝搬路の伝達関数を推定し、上記伝達関数の逆特性を実現する等化器を備え、
上記等化器で決定されたフィルタ係数に基づいて上記秘密鍵を生成する通信装置。
【請求項７】　請求項１、２、３または４において、
上記既知の信号がパイロットシンボルであり、上記伝搬路の遅延プロファイルまたは上記周波数特性を推定する手段は、内部にパイロットシンボルをそれぞれ含む、送信パケットと上記受信データパケットとが時間的に隣接して配され、上記受信データパケット中の上記パイロットシンボルを使用して上記遅延プロファイルまたは上記周波数特性を推定する通信装置。
【請求項８】　請求項１、２、３または４において、
上記既知の信号がパイロットシンボルであり、送信データパケットおよび受信データパケットにそれぞれ上記パイロットシンボルが含まれ、上記送信データパケットと上記受信データパケットとが時間的に隣接して配され、上記受信データパケット中の上記パイロットシンボルを使用して上記遅延プロファイルまたは上記周波数特性を推定する通信装置。
【請求項９】　請求項１、２、３または４において、
上記既知の信号がパイロットシンボルであり、送信および受信するデータパケットと別個に上記パイロットシンボルのスロットを形成し、送信するパイロットシンボルと受信するパイロットシンボルとを時間的に隣接したスロットに配し、受信したパイロットシンボルを使用して上記遅延プロファイルまたは上記周波数特性を推定する通信装置。
【請求項１０】　請求項１、２、３または４において、
上記既知の信号としてＰＮ系列を使用する通信装置。
【請求項１１】　請求項１、２、３または４において、
さらに、平文に対して第１の誤り検出符号で符号化を行い、第１の誤り検出符号のパリティを有するデータに対して暗号化を行い、暗号化されたデータに対して第２の誤り検出符号で符号化を行う通信装置。
【請求項１２】　請求項１、２、３または４において、
受信データは、送信側において、平文に対して第１の誤り検出符号で符号化がされ、上記第１の誤り検出符号のパリティを有するデータに対して暗号化がなされ、暗号化されたデータに対して第２の誤り検出符号で符号化がされており、
上記第２の誤り検出符号の復号化を行い、復号結果が合

格であれば、上記秘密鍵を使用して復号化を行い、上記第１の誤り検出符号の復号化を行い、復号結果が合格であれば、復号化データとして出力する通信装置。

【請求項１３】　略同一のキャリア周波数を時分割に使用して他の通信装置との間で送信および受信を交互に行なう無線通信システムにおける無線通信システムにおける通信方法において、

既知の信号に基づいて、上記他の通信装置との間の伝搬路の遅延プロファイルを推定するステップと、

推定した上記遅延プロファイルの複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成するステップと、

上記秘密鍵を用いて情報データを暗号化して送信し、または上記秘密鍵で暗号化された情報データを受信して復号化を行なうステップとを有する通信方法。

【請求項１４】　略同一のキャリア周波数を時分割に使用して他の通信装置との間で送信および受信を交互に行なう無線通信システムにおける通信方法において、

既知の信号に基づいて、上記他の通信装置との間の伝搬路の周波数特性を推定するステップと、

推定した上記周波数特性の複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成するステップと、

上記秘密鍵を用いて情報データを暗号化して送信し、または上記秘密鍵で暗号化された情報データを受信して復号化を行なうステップとを有する通信方法。

【請求項１５】　略同一のキャリア周波数を時分割に使用して他の通信装置との間で送信および受信を交互に行なう無線通信システムにおける通信方法であって、

ハードウェアの一部または全部がプログラム可能な論理回路で構成され、論理回路に対するプログラムデータによって、所望の無線通信方式を実現するようにした通信方法において、

既知の信号に基づいて、上記他の通信装置との間の伝搬路の遅延プロファイルを推定するステップと、

推定した上記遅延プロファイルの複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成するステップと、

上記秘密鍵を用いてプログラムデータを暗号化して送信し、または上記秘密鍵で暗号化されたプログラムデータを受信して復号化を行なうステップとを有する通信方法。

【請求項１６】　略同一のキャリア周波数を時分割に使用して他の通信装置との間で送信および受信を交互に行なう無線通信システムにおける通信方法であって、

ハードウェアの一部または全部がプログラム可能な論理回路で構成され、論理回路に対するプログラムデータによって、所望の無線通信方式を実現するようにした通信方法において、

既知の信号に基づいて、上記他の通信装置との間の伝搬路の周波数特性を推定するステップと、

推定した上記周波数特性の複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成するステップと、

上記秘密鍵を用いてプログラムデータを暗号化して送信し、または上記秘密鍵で暗号化されたプログラムデータを受信して復号化を行なうステップとを有する通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、無線通信システムにおける通信装置および通信方法に関する。

【０００２】

【従来の技術】近年、普及の著しい携帯電話や無線ＬＡＮ(Local area network)を始めとする移動体無線通信システムは社会の最も重要なインフラの一つと見なすことができる。当然のことであるが、例えば企業や情報機密および個人のプライバシー保護の観点から無線の盗聴を防止するためには暗号化は必須である。

【０００３】一方、近年、ソフトウェア無線通信システムの研究開発が活発に行なわれている。ソフトウェア無線通信システムとは、無線通信システムをディジタル化してソフトウェアでシステム機能を変更することにより、単一のハードウェアでも複数のシステム機能に対応できるマルチモードのシステムを実現するという概念である。ソフトウェア無線通信システムによれば、通信装置の仕様、規格、動作特性などを使用する環境に応じて変更することが可能となり、また、各種の通信方式や異なる規格がプログラムを書き換えるだけで一つの装置で使用できるようになるため、開発費用の削減、期間の短縮、大量生産及び、保守・更新への適合性、低コスト化を実現できる。

【０００４】より具体的には、ソフトウェア無線通信技術では、マイクロプロセッサやＤＳＰ(Digital Signal Processor)のチップまたはＦＰＧＡ(Field Programmable Gate Array)を用いてディジタル無線通信用のプログラマブルな変復調装置を構成し、所望の通信方式の変復調方式を構成するためのソフトウェアを変復調装置にインストールして、種々の仕様を同一のハードウェアで柔軟に実現することができる。例えばソフトウェアをインストールすることによって、ＰＨＳ(Personal Handyphone System)や携帯電話、構内ＬＡＮ(Local Area Network)等の異なる無線通信方式を１つの無線通信装置で実現することができれば、ユーザは同一の無線端末装置さえあればその地域の通信方式のプログラムをインストールすることによって世界中でサービスを受けられる。端末装置の製造メーカにとっては、ハードウェアを共通化することによって量産が可能となり、製造コストを削減できる。

【０００５】ところで、ソフトウェア無線通信システム

において、共通のハードウェア上に種々のプログラムを搭載して対応した無線通信方式に基づく無線通信装置を実現するためには、ソフトウェアのインストール方式としては、電話や、有線インターネット等の有線によってケーブルを接続してダウンロードする方法（第１の方法）、超小型のメモリデバイスによる方法（第２の方法）、無線によってプログラムをダウンロードする方法（第３の方法）が考えられる。

【０００６】第１の方法は、自宅、職場、販売店、駅・空港等の公共施設にソフトウェア供給装置を設けて利用者のソフトウェア無線端末装置をケーブルで接続して有線経由でダウンロードする方法である。第１の方法は、利用者はソフトウェア供給装置のある場所を探し、足を運ばなければならない問題点を有する。第２の方法は、販売店などで所望のソフトウェアが格納されているメモリデバイスを購入する必要がある。媒体であるメモリデバイスの価格分高くなってしまう。第３の方法は、前述した第１および第２の方法と異なり利用者が電波の届く場所にいれば、所望のプログラムを伝送して効率よくダウンロードできる。そこで、以降は無線経由でプログラムの伝送・ダウンロードを行なう無線ダウンロードの方式に着目する。

【０００７】ソフトウェア無線機が動作するのに必要とされるプログラムは、メーカが作成して政府の電波を管理する部署が電波法を満たすかどうかを検査して、その検査に合格し、販売を認可されたプログラムでなければならない。例えば、そのプログラムに意図的な改竄が行なわれた場合、インストールしたソフトウェア無線機が違法電波または妨害電波を発生してしまうことになり、無線通信インフラを破壊しかねない。あるユーザＡに対してソフトウェアの無線ダウンロードが行なわれると仮定する。悪意のある別のユーザＢがそのプログラムを盗聴しソフトウェア無線機にダウンロードしてユーザＡになりすまして通信を行なってしまうことも有り得る。この場合では、ユーザＡに経済的に多大な損害を与えることも考えられる。また、ユーザＢが盗聴したプログラムを改竄して違法電波を発生することも有り得る。

【０００８】以上のような情報データとソフトウェア無線通信システムにおけるプログラムの機密性を向上させるために、暗号化技術を適用する方法がある。従来の暗号化技術として、図１および図２に示すようなものが知られている。図１は一般的な公開鍵暗号方式の構成である。この方式の代表的な暗号はＲＳＡ(Rivest-Shamir-Adleman)暗号がある。公開鍵と秘密鍵はともに整数値である。公開鍵は一般に公開されているが、一方、秘密鍵は公開されないため、暗号通信に先立って第三者に盗聴されないように配送されなければならない。図１において、参照符号１ａが暗号通信で送信する予定の情報データまたはプログラムである。参照符号１ｂが暗号化アルゴリズムである。参照符号１ｃが伝送路であり、参照符号１ｄが受信側における復号化アルゴリズムであり、復号化アルゴリズム１ｄは、受信した暗号化を復号化鍵すなわち秘密鍵を用いて、参照符号１ｅで示す情報データまたはプログラムを復号化する。

【０００９】図２は、暗号化鍵および復号化鍵として、共に秘密鍵を使用する共通鍵方式または秘密鍵方式の構成を示す。この方式の代表的な例はＤＥＳ(Data EncryptionStandard)および、ＤＥＡ(Data Encryption Algorithm)であり、それぞれ、ＡＮＳＩ（米国規格協会、American National Standrds Institure)とＩ-ＳＯ（国際標準化機構、International Organization for Standardization)で標準化されている。秘密鍵は送信側と受信側で同じ鍵を持たなければならないので、通信のペアの両者に同じ鍵を持たせるために、暗号通信に先立って第三者に盗聴されないように鍵を配送しなければならない。参照符号２ａが暗号通信で送信する予定の情報データまたはソフトウェアである。参照符号２ｂが暗号化アルゴリズムである。参照符号２ｃは伝送路であり、参照符号２ｄは受信側における復号化アルゴリズムであり、復号化アルゴリズム２ｄは、受信した暗号化データを復号化鍵すなわち秘密鍵を用いて、参照符号２ｅで示す情報データまたはプログラムを復号化する。

【００１０】

【発明が解決しようとする課題】従来の暗号化技術例えば秘密鍵方式を使用して、ソフトウェア無線通信システムにおける基地局では、秘密鍵を用いてプログラムに対して暗号化を施した後に端末局に伝送する。端末局では秘密鍵を用いて復号化の後、プログラムをダウンロードする。しかしながら、端末局側の秘密鍵の番号が漏洩し、悪意のある利用者がその秘密鍵を用いて暗号を解読し、プログラムを解析し、改竄の後に端末のハードウェアにインストールして違法電波を送信し、無線インフラを破壊する可能性がある。したがって、現在、信頼性の高い秘密鍵生成方法の確立が必要であると考えられる。

【００１１】したがって、この発明の目的は、鍵配送の問題を生じることがなく、無線通信システムにおいて情報データ、ソフトウェア無線のプログラムデータ等を安全に通信することを可能とする通信装置および通信方法を提供することにある。

【００１２】

【課題を解決するための手段】上述した課題を解決するために、請求項１の発明は、略同一のキャリア周波数を時分割に使用して他の通信装置との間で送信および受信を交互に行なう無線通信システムにおける通信装置において、既知の信号に基づいて、他の通信装置との間の伝搬路の遅延プロファイルを推定する手段と、推定した遅延プロファイルの複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成する手段と、秘密鍵を用いて情報データを暗号化して送信し、または秘密鍵で暗号化された情報データを受信して復号化

を行なう手段とを有する通信装置である。請求項１３は、推定した遅延プロファイルの複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成する通信方法である。

【００１３】請求項２の発明は、略同一のキャリア周波数を時分割に使用して他の通信装置との間で送信および受信を交互に行なう無線通信システムにおける通信装置において、既知の信号に基づいて、他の通信装置との間の伝搬路の周波数特性を推定する手段と、推定した周波数特性の複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成する手段と、秘密鍵を用いて情報データを暗号化して送信し、または秘密鍵で暗号化された情報データを受信して復号化を行なう手段とを有する通信装置である。請求項１４の発明は、推定した周波数特性の複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成する通信方法である。

【００１４】請求項３の発明は、略同一のキャリア周波数を時分割に使用して他の通信装置との間で送信および受信を交互に行なう無線通信システムにおける通信装置であって、ハードウェアの一部または全部がプログラム可能な論理回路で構成され、論理回路に対するプログラムデータによって、所望の無線通信方式を実現するようにした通信装置において、既知の信号に基づいて、他の通信装置との間の伝搬路の遅延プロファイルを推定する手段と、推定した遅延プロファイルの複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成する手段と、秘密鍵を用いてプログラムデータを暗号化して送信し、または秘密鍵で暗号化されたプログラムデータを受信して復号化を行なう手段とを有する通信装置である。請求項１５の発明は、推定した遅延プロファイルの複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成する通信方法である。

【００１５】請求項４の発明は、略同一のキャリア周波数を時分割に使用して他の通信装置との間で送信および受信を交互に行なう無線通信システムにおける通信装置であって、ハードウェアの一部または全部がプログラム可能な論理回路で構成され、論理回路に対するプログラムデータによって、所望の無線通信方式を実現するようにした通信装置において、既知の信号に基づいて、他の通信装置との間の伝搬路の周波数特性を推定する手段と、推定した周波数特性の複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成する手段と、秘密鍵を用いてプログラムデータを暗号化して送信し、または秘密鍵で暗号化されたプログラムデータを受信して復号化を行なう手段とを有する通信装置である。請求項１６の発明は、推定した周波数特性の複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成する通信方法である。

【００１６】この発明では、電波伝搬路の遅延プロファイルまたは周波数特性が二つの通信装置の間で固有の情報となることに着目し、二つの通信装置間の伝搬路の遅延プロファイルまたは周波数特性から暗号化の秘密鍵を生成する。秘密鍵を相手に伝送する必要がなく、高いセキュリティで無線通信を行うことができる。情報シンボルデータのみならず、ソフトウェア無線装置のプログラムデータも高いセキュリティでもって通信できる。

【００１７】

【発明の実施の形態】この発明の一実施形態について以下説明する。基地局から端末局に情報データまたはプログラムを伝送する際に他局に盗聴されないような暗号用の秘密鍵を生成するためには、基地局と端末局の２者のみしか知らない固有の情報に着目すれば良い。ここで、基地局から端末局に対して送信される電波の下りのキャリアに周波数と端末局から基地局に対して送信される電波の上りのキャリア周波数は一致し、十分に短い時間間隔で上りと下りの電波が交互に繰り返されて送信されるものとする。

【００１８】波長が数ｃｍ（通常１GHz以上）のマイクロ波、または数ミリ程度（３０～３００GHz）のミリ波を使用した場合、基地局と端末局の無線伝搬路の伝達関数または周波数特性は、その時刻と位置に依存した両者に固有のデータと成り得る。空間的にたかだか数ｃｍの距離を移動するのみで無線伝搬路の特性が激変し、自己と周囲の移動物体によって特性は時々刻々と変動する。したがって、基地局と他の端末間の電波伝搬路の特性とは無相関であるとみなせるから、その無線伝搬路の特性から特徴量を抽出して、それに基づいて秘密鍵を生成すれば極めて機密性の高い暗号化を行うことができる。

【００１９】図３は、陸上移動通信における電波伝搬の様子を示す。基地局３ａと端末局３ｂ間には、建造物、自動車や樹木が存在する。これらは電波が伝搬するうえで大きな影響を与える。屋外の基地局３ａから送信された電波は唯一の通り道だけを通って伝搬するのではなく、あらゆる方向に放射され、移動局３ｂへ直接到来する直接波３ｃの他にビル３ｄによる反射波３ｅ、自動車３ｆなどの移動物体による反射波３ｇが端末局３ｂに到達する。２局間には他にも電波が建造物の角などにより電波の進行方向が曲げられる回折波、建造物の角や壁面の不均一性などで電波があらゆる方向に散っていく錯乱波も無数存在する。これらの電波はそれぞれに経路長が異なるため、移動局に到達する時間が異なる。その結果として移動局では到達時間の異なるいくつもの電波（遅延波）の重ね合わせを受信することになる。これをマルチパルスと呼ぶ。

【００２０】端末局や周囲の反射物が移動することにより激しいフェージングを伴った電波となる一般的な携帯電話のセルラ環境においては、フェージング特性がレイリー分布となることが解析的に導かれている。レイリー

フェージング下における受信信号の空間的な相関については空間で半波長程度離した２本のアンテナで受信したフェージング信号は互いに無相関であると導かれている。例えば、キャリア周波数をそれぞれ、２GHzと５GHzとすればλ＝１５０mm、λ＝６０mmであるから、無相関であるための空間的なアンテナの距離はそれぞれ、７５mmと３０mmとなる。

【００２１】電波の伝搬路特性は、時間領域で表される遅延プロファイルと、周波数特性で表現することができる。図４は、ある伝搬環境の遅延プロファイルの例を示す。遅延プロファイルは、基本的には、インパルス波形を地点Ａから送信し、地点Ｂで受信したインパルス波形の電力の過渡応答を測定したものである。これは、電波の伝搬路の時間領域の伝達特性を表す。最初に、時刻が０のときに最も遅延が最小で受信電力が最大の直接波が到来して、続いて電力の減衰した反射波・回折波・錯乱波が伝搬距離に応じて遅れて到来することを示している。

【００２２】マイクロ波とミリ波において、遅延プロファイルの波形は、受信地点とある時刻において固有の特性であり、数ミリから数センチのオーダーで離れた２つの受信地点で測定すれば、各受信地点における伝搬特性は無相関の異なった特性となる。つまり、伝搬路の遅延プロファイルの各時間に対応したパスの振幅と位相が異なる。この点に着目すれば、振幅と位相情報は、キャリア周波数、時刻、送信点並びに受信地点に固有のものであり、他の受信地点では得ることができない。したがって、この特性から基地局と端末局のみが共有する秘密鍵を生成することが可能となる。また、時間領域上の特性である遅延プロファイルを周波数領域に変換した周波数特性においても同様である。

【００２３】インパルス波形は広帯域のスペクトラムを有するために他の無線通信に妨害を与えてしまうおそれがある。そこで、インパルス波を送信する代わりに、キャリアを自己相関特性の強い既知のＰＮ(Pseudo Noise)信号（M系列とも呼ばれる）で変調し、被変調信号を送信する。受信側では、受信信号と同一のＰＮ信号との相関演算を行なう。遅延プロファイルは、このような手法で測定することができる。

【００２４】図５は、遅延プロファイル測定のための送信装置の構成例を示す。参照符号５ａで示すＰＮ系列発生器５ａは、シフトレジスタと排他的論理和ゲートから構成されている。ＰＮ系列の出力ビットがＢＰＳＫ(Binary Phase Shift Keying:２相位相偏移変調）変調器５ｂによってＢＰＳＫ変調される。ＢＰＳＫ変調器５ｂの出力のＩチャンネル（同相成分）のディジタルデータＩ－ＤとＱチャンネル（直交成分）のディジタルデータＱ－ＤがそれぞれＤ／Ａ変換器５ｃによってベースバンドアナログ信号に変換される。直交検波器５ｄにおいて、ベースバンドアナログ信号が第１局部発振器５ｅの発振周波数の中間周波数帯信号に変換される。その後に送信ミキサ５ｆと第２局部発振器５ｇによってキャリア周波数に変換され、パワーアンプ５ｈで電力増幅を行なった後にアンテナ５ｉから送信される。

【００２５】図６は、遅延プロファイル測定のための受信装置の構成例を示す。ディジタル変調されたキャリアをアンテナ６ａより受信し、ローノイズアンプ６ｂで受信波の信号増幅を行なう。ローノイズアンプ６ｂの出力信号が受信ミキサ６ｃに供給され、受信ミクサ６ｃにおいて、第１局部発振器６ｄの出力信号と乗積されることによって中間周波数帯信号に変換される。直交検波器６ｅと第２局部発振器６ｆによって中間周波数帯信号は、ＩチャンネルとＱチャンネルから構成されるベースバンド信号に変換される。Ａ／Ｄ変換器６ｇによって両チャンネルのベースバンドアナログ信号がそれぞれディジタルデータに変換される。各チャンネルのディジタルデータが複素数相関器６ｈに入力される。送信装置で使用されたのと同種のＰＮ発生器６ｉがＢＰＳＫ変調器６ｊによって変調され、ＢＰＳＫ変調器６ｊからのディジタル変調信号と受信信号との複素数相関演算が複素数相関器６ｈにおいて行われ複素遅延プロファイとして出力される。

【００２６】図７は、測定された複素遅延プロファイルの一例を示す。各グラフの横軸は遅延時間を表す。図７Ａおよび図７Ｂは、それぞれ複素遅延プロファイルの振幅の実数成分の時系列データ７ａと虚数成分の時系列データ７ｂを示す。図７Ｃおよび図７Ｄは、それぞれ複素数の振幅情報から計算した電力の時系列データ７ｃと位相の時系列データ７ｄを示す。

【００２７】次に、電波の伝搬路の周波数特性について説明する。周波数特性は、図７Ａおよび図７Ｂに示すような複素遅延プロファイルの振幅の時系列複素数データをＤＦＴ(Discrete Fourier Transform)またはＦＦＴ(Fast Fourier Transform)によって周波数領域の複素数データに変換したものである。図８は、ＦＦＴを使用した場合の計算手法を示す。図６に示した受信装置の複素遅延プロファイルの出力をシリアル・パラレル変換器８ａによってＦＦＴのポイント数のパラレルデータに変換してＦＦＴ８ｂに入力する。ＦＦＴ８ｂが伝搬路の周波数特性を出力する。なお、図面において、実線の信号経路が実数データの信号経路を表し、破線の信号経路が虚数データの信号経路を表している。

【００２８】以上の説明では、図５に示した送信装置と、図６に示した受信装置とを使用した自己相関特性の良好なＰＮ信号を使用した遅延プロファイルの測定システムについて説明した。次に、ＰＮ信号を使用しない一般的な既知信号を使用した伝搬路の周波数特性の測定手法について述べる。送信側では、図５のＰＮ発生器５ａとＢＰＳＫ変調器５ｂの代わりにディジタル変調された既知信号が生成され、既知信号が送信される。

【００２９】一方、受信側では、Ａ／Ｄ変換された複素ディジタルデータに対して、図６中の複素数相関器６ｈ、ＰＮ発生器６ｉ、ＢＰＳＫ変調器６ｊに代えて図９に示す構成が設けられる。受信した時間領域の既知信号の複素ディジタルデータｘ(t)がシリアル・パラレル変換器９ａによってパラレルデータに変換され、ＦＦＴ９ｂによって周波数領域のパラレルデータＸ(f)に変換される。あらかじめ用意した既知信号データｙ(t)９ｃがシリアル・パラレル変換器９ｄによってパラレルデータに変換され、変換したパラレルデータをＦＦＴ９ｅに入力して周波数領域データＹ(f)に変換する。Ｘ(f)をＹ(f)で複素除算することによって伝搬路の周波数特性Ｚ(f)を求めることができる。すなわち、Ｙ(f)Ｚ(f)＝Ｘ(f)の関係にあり、Ｚ(f)＝Ｘ(f)／Ｙ(f)となる。

【００３０】図１０は、伝搬路の周波数特性の例を示す。各グラフの横軸は周波数を示す。図１０Ａおよび図１０Ｂは、それぞれ振幅の実数成分１０ａと虚数成分１０ｂを示す。図１０Ｃおよび図１０Ｄは、複素振幅のデータから計算した電力の特性１０ｃと位相の特性１０ｄをそれぞれ示す。

【００３１】図７に示した複素遅延プロファイルと、図１０に示した伝搬路の周波数特性は、例えば、５ＧＨｚのキャリア周波数を使用して測定したとすれば、受信アンテナの空間的な距離が３０ｍｍ以上離れていればそれぞれの受信地点での特性は無相関であるとみなせる。また受信地点と送信地点を交換しても同一周波数で且つ測定時刻が十分に近ければ可逆性が成立し、送信側と受信側のアンテナや増幅器などの利得を考慮して正規化すれば同様な特性が得られる。したがって、伝搬路の複素遅延プロファイルと周波数特性は送信側と受信側の両者だけのキャリア周波数と位置と時刻に依存する固有の特性であるとみなせる。それらの特性をある手法に基づいて数値化すれば、送信側と受信側が共有する秘密鍵を生成することが可能となる。以下に、伝搬路の遅延プロファイルと周波数特性の電力、振幅、位相の各情報による秘密鍵生成の手法を示す。

【００３２】図１１は、電力情報から秘密鍵を生成する構成を示す。遅延プロファイルまたは周波数特性の電力のパラレルデータがＭ入力Ｎ出力選択器１１ａに入力される。Ｍ入力Ｎ出力選択器１１ａは、Ｍ個の遅延プロファイルまたは周波数特性の複素パラレルデータの中で、電力が比較的大きいＮ個のデータを選択して出力する。図７の遅延プロファイルの例では、t_0, t_1, t_2, ・・・, t_Mのそれぞれの時刻のそれぞれの振幅がＭ個のデータである。この選択器１１ａで選択されたＮ個の遅延プロファイルまたは周波数特性の複素パラレルデータが電力・秘密鍵生成器１１ｂに入力されて秘密鍵が生成される。

【００３３】図１２は、振幅情報から秘密鍵を生成する構成を示す。遅延プロファイルまたは周波数特性の振幅のパラレルデータがＭ入力Ｎ出力選択器１２ａに入力される。Ｍ入力Ｎ出力選択器１２ａは、Ｍ個の遅延プロファイルまたは周波数特性の複素パラレルデータの中で、電力が比較的大きいＮ個のデータを選択して出力する。この選択器１２ａで選択されたＮ個の遅延プロファイルまたは周波数特性の複素パラレルデータが電力・秘密鍵生成器１２ｂに入力されて秘密鍵が生成される。

【００３４】図１３は、位相情報から秘密鍵を生成する構成を示す。遅延プロファイルまたは周波数特性の位相のパラレルデータがＭ入力Ｎ出力選択器１３ａに入力される。Ｍ入力Ｎ出力選択器１３ａは、Ｍ個の遅延プロファイルまたは周波数特性の複素パラレルデータの中で、電力が比較的大きいＮ個のデータを選択して出力する。この選択器１３ａで選択されたＮ個の遅延プロファイルまたは周波数特性の複素パラレルデータが電力・秘密鍵生成器１３ｂに入力されて秘密鍵が生成される。

【００３５】図１４は、Ｍ入力Ｎ出力選択器の構成例を示す。Ｍ≧Ｎとする。Ｍ個の入力複素数データはそれぞれ電力計算回路$14a_1$～$14a_M$に入力されて電力が計算される。例えば入力データ番号が１の入力データの実数データa_1と虚数データb_1とから、電力計算回路$14a_1$は、$(a_1^2+b_1^2)$の演算によって電力を計算する。計算した電力値がマルチプレクサ制御信号生成器１４ｂに入力されて電力の比較的高いＮ個の入力複素数データを選択する制御信号が生成される。この制御信号がＮ個のマルチプレクサ$14c_1$～$14c_N$に供給される。マルチプレクサ$14c_1$～$14c_N$に対しては、Ｍ個の入力複素数データが供給され、制御信号にしたがってその中の一つが選択的に出力される。マルチプレクサ$14c_1$～$14c_N$によって選択したＮ個の入力複素数データが出力される。

【００３６】図１１、図１２、図１３にそれぞれ示された電力情報、振幅情報、位相情報から秘密鍵を生成する秘密鍵生成器１１ｂ，１２ｂ，１３ｂの構成についてさらに説明する。

【００３７】図１５は、電力・秘密鍵生成器１１ｂの構成例を示す。Ｎ個の複素数データはそれぞれ電力計算回路$15a_1$～$15a_N$によって電力が計算される。計算した電力値は多入力加算器１５ｂに入力され電力和が求められる。その電力和に対して除算器１５ｃによってデータ個数Ｎで除算が行われて平均電力が算出される。この平均電力値を用いて各入力データの電力値を除算器$15d_1$～$15d_N$でそれぞれ除算して正規化を行なう。正規化した各データに対して量子化回路$15e_1$～$15e_N$によって量子化が行われ、それぞれｐビットのビット系列に割り当てられる。入力されたＮ個のビット系列はビット結合器１５ｆによって結合されてＮｐビットの秘密鍵として出力される。

【００３８】図１６は、図１５で使用した電力計算回路$15a_1$～$15a_N$の構成例を示す。入力された実数デー

タと虚数データを２乗回路１６ａ，１６ｂでそれぞれ２乗した後に加算器１６ｃで加算して電力値として出力する。

【００３９】図１７は、図１５で使用した量子化回路１５e_1～１５e_Nの動作例を示す。ここではｐ＝３、すなわち、３ビット出力の例を示す。入力された正規化された電力値に対応するビット系列を出力する。レベル範囲の境界上の白い丸は、その値を範囲内に含まないことを意味し、黒い丸は、その値を範囲内に含むことを意味する。例えば、正規化電力値として４．５が入力された場合、出力ビット系列として（１０１）が出力される。

【００４０】図１８は、ビット結合器の構成例を示す。量子化されて変換されたＮ個のデータ系列のビット数をそれぞれｐとすれば、それらを結合してＮｐビットのデータとして出力される。例えば、ｐ＝３として１番目のデータを（１００）、２番目のデータを（００１）、３番目のデータを（０１０）、Ｎ番目のデータを（１１１）とすれば、ビット結合器の出力は（１０００１０１０，…，１１１）となる。

【００４１】図１９は、図１２で使用した振幅・秘密鍵生成器１２ｂの構成例を示す。Ｎ個の複素振幅データの実数成分が多入力加算器１９ａに入力され、多入力加算器１９ａによって実数成分の振幅値の総和が求められ、また、虚数成分が多入力加算器１９ｂに入力され、多入力加算器１９ａによって虚数成分の振幅値の総和が求められる。実数成分の総和が除算器１９ｃに供給され、虚数成分の総和が除算器１９ｄに供給され、各除算器１９ｃ，１９ｄによって各総和をデータ入力数Ｎで割って実数と虚数のそれぞれの平均振幅値が求められる。

【００４２】求めた平均振幅値によって実数入力データと虚数入力データがそれぞれ正規化される。除算器１９e_1～１９e_Nによって、Ｎ個の実数入力データのそれぞれが実数成分の平均振幅値で除算されることで、正規化がなされる。同様に、除算器１９f_1～１９f_Nによって、Ｎ個の虚数入力データのそれぞれが虚数成分の平均振幅値で除算されることで、正規化がなされる。正規化された実数データが実数の量子化回路１９g_1～１９g_Nによってｐビットのビット系列にそれぞれ変換され、ビット結合器１９ｉに入力される。同様に、正規化された虚数データが虚数の量子化回路１９h_1～１９h_Nによってｐビットのビット系列にそれぞれ変換され、ビット結合器１９ｉに入力される。実数データおよび虚数データがビット結合器１９ｉによって結合されて２Ｎｐビットの秘密鍵として出力される。なお、図１９における量子化回路とビット結合器の構成は、図１７と図１８で示した構成とそれぞれ同様である。

【００４３】図２０は、位相・秘密鍵生成器１３ｂの構成例を示す。Ｎ個の複素数データはそれぞれ位相・ビット変換器２０a_1～２０a_Nによって位相値からｐビットのビット系列に変換されてビット結合器２０ｂに入力されて結合されたＮｐビットのビット系列が秘密鍵として出力される。ビット結合器の構成は図１８と同様である。図２０で図示はしないが、Ｎ個の複素数データから直接、位相・ビット変換する手法のほかに、例えば入力データ番号が１の複素数データの位相を基準位相θ_{ref}と定め、Ｎ個の複素数データから求めた位相値からθ_{ref}を引いた相対的な位相値を用いてビットに変換する手法も考えられる。

【００４４】図２１は、位相・ビット変換器２０a_1～２０a_Nの動作例を示す。図２１Ａに示す例では、入力された複素数データを（ｐ＝１）ビットに変換する例である。位相をθとすると、（$\pi/2<\theta\leq\pi$，$-\pi/2\leq\theta<-\pi$）では、θが０に変換され、（$0<\theta\leq\pi/2$，$-\pi/2<\theta\leq 0$）では、θが０に変換される。図２１Ｂに示す例では、実数軸（横軸）および虚数軸（縦軸）で表される２次元領域の４つの象限に含まれる位相がそれぞれ（ｐ＝２）ビットへ変換される。図２１Ｃに示す例では、２次元領域が４５°の各間隔で８個の領域に分割され、各領域に含まれる位相がそれぞれ（ｐ＝３）ビットへ変換される。なお、図２１Ｂと図２１Ｃにおいて、黒い丸はその境界を範囲内に含むことを意味し、白い丸はその値を範囲内に含まないことを意味する。

【００４５】上述したように、遅延プロファイルと伝搬路の周波数特性が測定（推定）され、測定（推定）された遅延プロファイルまたは伝搬路周波数特性から秘密鍵が生成される。次に、無線通信装置に対して、これらの手法を適用した例について説明する。

【００４６】図２２は、上述した秘密鍵生成方式によるソフトウェア無線通信装置の構成例を示す。上部は復調部、下部は変調部である。本構成では、情報データのみならず所望の変復調器を構成するためのプログラムをも暗号化して無線伝送を行なう。プログラムの暗号化と暗号復号化のための秘密鍵をこの発明による方式で生成するものとする。復調部では、アンテナ２２ａから受信された信号はアンテナスイッチ２２ｂを通り、ローノイズアンプ２２ｃに入力される。ローノイズアンプ２２ｃから出力された信号は、受信ミキサ２２ｅにおいて、第１局部発振器２２ｄの局部発振信号によって中間周波数帯信号に変換される。

【００４７】中間周波数帯信号は、直交検波器２２ｇにおいて、第２局部発振器２２ｆの出力信号により直交検波され、アナログベースバンド信号Ｉ、Ｑに変換される。アナログベースバンド信号Ｉ、Ｑは、Ａ／Ｄ変換器２２ｈにおいて、ディジタルベースバンド信号Ｉ－Ｄ、Ｑ－Ｄに変換される。ディジタルベースバンド信号Ｉ－Ｄ、Ｑ－Ｄがデマルチプレクサ２２ｉに供給される。ディジタルベースバンド信号Ｉ－Ｄ、Ｑ－Ｄがデマルチプレクサ２２ｉを介してベースバンド復調・暗号復号化・秘密鍵生成部２２ｊまたはプログラマブル復調部２２ｏ

に供給される。

【００４８】ベースバンド復調・暗号復号化・秘密鍵生成部２２ｊにおいては、復調・誤り訂正符号の復号化、さらに、暗号化と暗号復号化のための秘密鍵が生成され、暗号の復号化が行われてデマルチプレクサ２２１を通って情報データまたは変復調プログラムとして出力される。復調された変復調プログラムは、マルチプレクサ２２ｍを介してプログラマブル復調部２２ｏとプログラマブル変調部２２ｐに供給され、復調された変復調プログラムにしたがって、所望の仕様の変復調器が構成される。さらに、生成された秘密鍵はレジスタ２２ｋに記憶される。

【００４９】次に変調部の動作を説明する。マルチプレクサ２２ｑから出力される情報データまたはプログラムは、先ず、既に生成した秘密鍵が保持されているレジスタ２２ｋから秘密鍵を読み出して、暗号化・ベースバンド変調部２２ｒにおいて暗号化、誤り訂正符号化、ディジタル変調の処理を受ける。暗号化・ベースバンド変調部２２ｒは、ベースバンドディジタルデータとしてＩ－ＤとＱ－Ｄを出力する。これらのデータは、マルチプレクサ2.2ｓを介してＤ／Ａ変換器２２ｔによってそれぞれ、ベースバンドアナログＩ，Ｑ信号に変換される。

【００５０】アナログ信号は、第2局部発振器２２ｆの発振周波数の中間周波数帯に直交変調器２２ｕによって変換される。中間周波数帯のアナログ信号は、送信ミキサ２２ｖに供給され、送信ミキサ２２ｖにおいて、第１局部発振器２２ｄの発振周波数が加算されることで所望のキャリア周波数帯に変換される。この信号が電力増幅器２２ｗによって電力が増幅された後にアンテナスイッチ２２ｂを通りアンテナ２２ａによって送信される。

【００５１】プログラマブル変調部２２ｐとプログラマブル復調部２２ｏは、ディジタル信号処理をプログラムで行なうＤＳＰ(Digital signal processor)とプログラム可能な論理回路であるＦＰＧＡ(Field programmable gate arrays)から構成されている。プログラマブル変調部２２ｐとプログラマブル復調部２２ｏの機能を拡張することが可能で、ディジタル変復調のみならず、誤り訂正符号化・復号化機能や暗号化・暗号復号化機能も実現可能である。マルチプレクサ２２ｉ，２２ｓを制御することによって、ベースバンド復調・暗号復号化・秘密鍵生成部２２ｊと暗号化・ベースバンド変調部２２ｒの代わりにこれらのプログラマブルな変調部と復調部が前述した機能を実現することもできる。

【００５２】また、変復調プログラムデータベース２２ｎには、自己で使用するプログラムと相手局に無線で伝送するプログラムが格納されている。マルチプレクサ２２ｍは、プログラマブル変調部２２ｐと復調部２２ｏに対して無線伝送されたプログラムとデータベースのプログラムのどちらをダウンロードするかを選択する。マルチプレクサ２２ｑは、情報データとデータベースのプログラムのどちらを送信するかを選択する。なお、プログラムは、基地局に限らず、端末局が送信する機能を持つことも可能である。また、変復調プログラムデータベース２２ｎを基地局のみが備えていても良い。

【００５３】図２３は、暗号化・ベースバンド変調部２２ｒの構成例を示す。情報データ入力または変復調プログラム入力が暗号化器２３ａによって暗号化され、誤り訂正符号化器２３ｂによって符号化される。誤り訂正符号化器２３ｂの出力がマルチプレクサ２３ｃを介してベースバンドディジタル変調部２３ｄに供給され、変調部２３ｄによってディジタル変調され、ベースバンドディジタル変調データＩ－ＤとＱ－Ｄが出力される。

【００５４】伝搬路の遅延プロファイルと周波数特性の推定を行なうために、マルチプレクサ２３ｃには、パイロットシンボルが入力され、一定周期でパイロットシンボルが挿入されたデータがディジタル変調される。ベースバンドディジタル変調方式は、例えば、無線ＬＡＮで使用されているＯＦＤＭ(Orthogonal frequency-division multiplexing)変調方式、スペクトル拡散変調方式さらに、一般の携帯電話等で使用されているシングルキャリア変調方式等である。なお、図２３では、パケット生成ブロック等の図示を省略した。

【００５５】以下では、図２３におけるベースバンド復調・暗号復号化・秘密鍵生成部２２ｊの内部構成に関して、ＯＦＤＭ変調方式、スペクトル拡散変調方式、シングルキャリア変調方式の３種類の方式について説明を行なう。

【００５６】図２４にこの発明による秘密鍵生成器を搭載したＯＦＤＭ用ベースバンド復調・暗号復号化・秘密鍵生成部の第１の構成例を示す。図２４中のスイッチ２４ｅ、２４ｆは、それぞれ伝搬路特性推定モードと復調モードとで切り換えるものである。つまり、スイッチ２４ｅ、２４ｆが復調モードでは、１の状態とされ、伝搬路特性推定モードでは、２の状態とされる。切り換え信号は、省略されているが、制御部から各スイッチに供給される。スイッチ２４ｅ、２４ｆによって、ＦＦＴを伝搬路特性推定モードと復調モードとで兼用できる。

【００５７】入力されたベースバンド複素ディジタルデータに対してパケットタイミング同期部２４ａでタイミングの同期をとり、同期パルスを各部に供給する。また、入力されたベースバンドディジタルデータに対してキャリア周波数同期部２４ｂにおいてキャリア周波数を同期させる。同期させた後にシリアル・パラレル変換器２４ｃにおいてシリアルデータからＦＦＴの演算ポイント数の個数のパラレル複素数データに変換される。ＦＦＴ２４ｄにおいて入力された信号を周波数領域に変換し、周波数領域の信号をスイッチ２４ｅ，２４ｆに供給する。

【００５８】スイッチ２４ｅ，２４ｆが１の状態では、通常のＯＦＤＭ復調処理を行なう。スイッチが２４ｅ，

２４ｆが２の状態では、受信した信号からパイロットシンボルを抽出して伝搬路の周波数特性の推定を行なう。伝搬路周波数特性の推定手法は図９に説明した手法を使用している。パイロットシンボルは既知であるから同様にパイロットシンボルをあらかじめＦＦＴによって周波数領域に変換した参照データ２４ｈが具備されている。

【００５９】受信したパイロットシンボルをＦＦＴ２４ｄによって変換された周波数領域の信号に対して、複素数除算器２４ｇによって除算を行ない、伝搬路の周波数特性を計算する。その周波数特性から秘密鍵生成器２４ｉによって秘密鍵を生成してレジスタ２４ｋに記憶させる。この秘密鍵生成器２４ｉは、図１１、図１２および、図１３に示した構成に対応する。秘密鍵の生成手法は、図１１から図２２において説明したものである。周波数特性はレジスタ２４ｊに記憶される。

【００６０】スイッチ２４ｅ，２４ｆが１の状態では、このレジスタ２４ｊに記憶された伝搬路周波数特性を利用して等化器（複素数除算器）２４１において等化が行われる。等化器２４１の出力がパラレル・シリアル変換器２４ｍによってシリアルデータに変換されて誤り訂正符号復号化器２４ｎに供給されて誤り訂正符号の復号化が行われる。さらに、生成した秘密鍵を用いて暗号復号化器２４ｏにおいて暗号が復号化された後に情報ビットが出力される。また、生成した秘密鍵は変調部に出力される。

【００６１】図２５にはこの発明による秘密鍵生成器を搭載したＯＦＤＭ用ベースバンド復調・暗号復号化・秘密鍵生成部の第２の構成例を示す。入力されたベースバンド複素ディジタルデータに対しパケットタイミング同期部２５ａでタイミングの同期をとり、同期パルスを各部に供給する。また、入力されたベースバンドディジタルデータに対してキャリア周波数同期部２５ｂにおいてキャリア周波数を同期させる。同期させた後にシリアル・パラレル変換器２５ｃにおいてシリアルデータからＦＦＴの演算ポイント数の個数のパラレル複素数データに変換される。ＦＦＴ２５ｄにおいて入力された信号が周波数領域の複素数データに変換される。このデータは等化器２５ｅによって等化が行われた後にパラレル・シリアル変換器２５ｆにおいてシリアルデータに変換される。そして、誤り訂正符号復号化器２５ｇによって誤り訂正が行なわれ、その後に暗号復号化器２５ｈに供給される。暗号復号化器２５ｈでは、あらかじめレジスタ２５ｍに記憶した秘密鍵を使用して暗号の復号化が行われ、情報ビットが出力される。

【００６２】次に秘密鍵の生成について説明する。受信したパイロットシンボルは複素数相関器２５ｊにおいてあらかじめ具備されている共役パイロットシンボル２５ｉと相関演算が行われる。共役は、虚数部の符号が反転した関係を意味する。演算結果が遅延プロファイルとなる。遅延プロファイルのデータはシリアル・パラレル変換器２５ｋにおいてパラレル複素数データに変換された後に秘密鍵生成器２５１に供給される。秘密鍵生成器２５１によって秘密鍵が生成される。この生成器の構成は図１１、図１２および、図１３に示した構成例に対応する。生成した秘密鍵がレジスタ２５ｍに記憶されて、暗号復号化器２５ｈと変調部へ出力される。

【００６３】図２６にはこの発明による秘密鍵生成器を搭載したスペクトル拡散方式用ベースバンド復調・暗号復号化・秘密鍵生成部の第１の構成例を示す。入力されたベースバンド複素ディジタルデータに対してパケットタイミング同期部２６ａでタイミングの同期をとり、同期パルスを各部に供給する。また、入力されたベースバンド複素ディジタルデータに対してキャリア周波数同期部２６ｂにおいてキャリア周波数を同期させる。同期させた後、逆拡散・等化器２６ｃによって逆拡散と等化が行われる。その出力に対して誤り訂正符号復号化器２６ｄによって誤り訂正符号の復号化が行われて、暗号復号化器２６ｅにおいてあらかじめ生成されたレジスタ２６ｊに記憶されている秘密鍵を用いて暗号の復号化が行われて情報ビットが出力される。

【００６４】次に、秘密鍵の生成について説明する。ベースバンド複素ディジタルデータよりパイロットシンボルを抽出する。受信したパイロットシンボルは複素数相関器２６ｇにおいてあらかじめ具備されている参照パイロットシンボル２６ｆと相関演算が行われる。演算結果が遅延プロファイルとなる。遅延プロファイルのデータがシリアル・パラレル変換器２６ｈにおいてパラレルデータに変換された後に秘密鍵番号生成器２６ｉによって秘密鍵が生成される。この生成器の構成は図１１、図１２および、図１３に示した構成例に対応する。生成した秘密鍵はレジスタ２６ｊに記憶されて、暗号復号化器２６ｅと変調部へ出力される。また、推定した遅延プロファイルは逆拡散・等化器２６ｃにも供給される。

【００６５】図２７にはこの発明による秘密鍵生成器を搭載したスペクトル拡散方式用ベースバンド復調・暗号復号化・秘密鍵生成部の第２の構成例を示す。入力されたベースバンド複素ディジタルデータに対してパケットタイミング同期部２７ａでタイミングの同期をとり、同期パルスを各部に供給する。また、入力されたベースバンド複素ディジタルデータに対してキャリア周波数同期部２７ｂにおいてキャリア周波数を同期させる。同期させた後、逆拡散・等化器２７ｃによって逆拡散と等化が行われる。その出力に対して誤り訂正符号復号化器２７ｄによって誤り訂正符号の復号化が行われて、暗号復号化器２７ｅにおいてあらかじめ生成されレジスタ２７ｋに記憶されている秘密鍵を用いて暗号の復号化が行われて情報ビットが出力される。

【００６６】次に、秘密鍵の生成について説明する。ベースバンド複素ディジタルデータよりパイロットシンボルを抽出する。受信したパイロットシンボルは複素数相

関器２７ｇにおいてあらかじめ具備されている共役パイロットシンボル２７ｆと相関演算が行われる。演算結果が遅延プロファイルとなる。遅延プロファイルのデータがシリアル・パラレル変換器２７ｈにおいてＦＦＴポイント数のパラレルデータに変換される。そのパラレルデータはＦＦＴ２７ｉによって周波数領域に変換されて伝搬路の周波数特性が計算される。伝搬路の周波数特性から秘密鍵生成器２７ｊによって秘密鍵が生成される。その生成器の構成は図１１、図１２および図１３に示した構成に対応する。生成した秘密鍵はレジスタ２７ｋに記憶されて、暗号復号化器２７ｅと変調部へ出力される。また、推定した遅延プロファイルは逆拡散・等化器２７ｃにも供給される。

【００６７】図２８にはこの発明による秘密鍵生成器を搭載したシングルキャリア方式用ベースバンド復調・暗号復号器・秘密鍵生成部の第１の構成例を示す。入力されたベースバンド複素ディジタルデータに対してバケットタイミング同期部２８ａでタイミングの同期をとり、同期パルスを各部に供給する。また、入力されたベースバンドディジタルデータに対してキャリア周波数同期部２８ｂにおいてキャリア周波数を同期させる。同期させた後、等化器２８ｃによって等化が行われる。その出力に対して誤り訂正符号復号化器２８ｄによって誤り訂正符号の復号化が行われて、暗号復号化器２８ｅにおいてあらかじめ生成されレジスタ２８ｊに記憶されている秘密鍵を用いて暗号の復号化が行われて情報ビットが出力される。

【００６８】次に、秘密鍵の生成について説明する。ベースバンド複素ディジタルデータよりパイロットシンボルを抽出する。受信したパイロットシンボルは複素数相関器２８ｇにおいてあらかじめ具備されている共役パイロットシンボル２８ｆと相関演算が行われる。演算結果が遅延プロファイルとなる。遅延プロファイルのデータはシリアル・パラレル変換器２８ｈにおいてパラレルデータに変換された後に秘密鍵生成器２８ｉによって秘密鍵が生成される。この生成器の構成は図１１、図１２および、図１３に示した構成に対応する。生成した秘密鍵はレジスタ２８ｊに記憶されて、暗号復号化器２８ｅと変調部へ出力される。また、推定した遅延プロファイルは等化器２８ｃにも供給される。

【００６９】図２９にはこの発明による秘密鍵生成器を搭載したシングルキャリア方式用ベースバンド復調・暗号復号化・秘密鍵生成部の第２の構成例を示す。入力されたベースバンド複素ディジタルデータに対してバケットタイミング同期部２９ａでタイミングの同期をとり、同期パルスを各部に供給する。また、入力されたベースバンドディジタルデータに対してキャリア周波数同期部２９ｂにおいてキャリア周波数を同期させる。同期させた後、等化器２９ｃによって等化が行われる。その出力に対して誤り訂正符号復号化器２９ｄによって誤り訂正符号の復号化が行われて、暗号復号化器２９ｅにおいてあらかじめ生成されレジスタ２９ｋに記憶されている秘密鍵を用いて暗号の復号化が行われて情報ビットが出力される。

【００７０】次に、秘密鍵の生成について説明する。ベースバンド複素ディジタルデータよりパイロットシンボルを抽出する。受信したパイロットシンボルは複素数相関器２９ｇにおいてあらかじめ具備された共役パイロットシンボル２９ｆと相関演算が行われる。演算結果が遅延プロファイルとなる。遅延プロファイルのデータはシリアル・パラレル変換器２９ｈにおいてパラレルデータに変換される。そのパラレルデータがＦＦＴ２９ｉによって周波数領域に変換されて伝搬路の周波数特性が計算される。伝搬路周波数特性から秘密鍵生成器２９ｊによって秘密鍵が生成される。この生成器の構成は図１１、図１２および、図１３に示した構成に対応する。生成した秘密鍵はレジスタ２９ｋに記憶されて、暗号復号化器２９ｅと変調部へ出力される。また、推定した遅延プロファイルは等化器２９ｃにも供給される。

【００７１】図３０にはこの発明による秘密鍵生成器を搭載したシングルキャリア方式用ベースバンド復調・暗号復号化・秘密鍵生成部の第３の構成例を示す。入力されたベースバンド複素ディジタルデータに対してバケットタイミング同期部３０ａでタイミングの同期をとり、同期パルスを各部に供給する。また、入力されたベースバンドディジタルデータに対してキャリア周波数同期部３０ｂにおいてキャリア周波数を同期させる。同期させた後、等化器３０ｃによって等化が行われる。その出力が誤り訂正符号復号化器３０ｄによって誤り訂正符号の復号化が行われて、暗号復号化器３０ｅにおいてあらかじめ生成されたレジスタ３０ｇに記憶された秘密鍵を用いて暗号の復号化が行われて情報ビットが出力される。

【００７２】次に、秘密鍵の生成について説明する。一般的な等化器は、内部にパイロットシンボルを具備し、そのシンボルを使用してある種の推定アルゴリズムによって伝搬路の伝達関数を推定し、その伝達関数の逆特性をＦＩＲ(Finite Impulse Response)フィルタで実現し誤差が最小となるようにフィルタの係数を適応的に決定している。また、そのフィルタの係数は、その時刻における伝搬路の固有なパラメータであると考えられる。そこで、等化器３０ｃのフィルタの係数データを秘密鍵生成器３０ｆに供給して秘密鍵を生成する。その生成器の構成は図１１、図１２および、図１３に示した構成に対応する。生成した秘密鍵はレジスタ３０ｇに記憶されて、暗号復号化器３０ｅと変調部へ出力される。

【００７３】図３１に図３０の構成図内で使用する等化器３０ｃの構成例を示す。等化器に供給された入力複素数データがレジスタ３１a_1～３１a_{M-1}が縦続接続されたシフトレジスタにサンプリングクロック毎に記憶される。レジスタ３１a_1～３１a_{M-1}の入力データおよび出

力データが係数生成部３１ｃと複素数乗算器３１b_1～３１b_Mに供給される。係数生成部３１ｃでは、ＬＭＳ(Least Mean Squares)アルゴリズムまたは、ＲＬＳ(Recursive Least Squares)アルゴリズムによって係数が生成される。

【００７４】係数生成部３１ｃで生成された係数が複素乗算器３１b_1～３１b_Mに供給され、計数出力C_1～C_Mとレジスタ３１a_1～３１a_{M-1}の入出力データとの積が生成される。この積が複素数多入力加算器３１ｄに入力される。加算器３１ｄの出力がスイッチ３１ｅ，３１ｆに入力される。スイッチ３１ｅ，３１ｆが１の状態に設定された場合では、通常の等化器として動作が行われ、等化された結果として出力される。一方、パイロットシンボルを受信・入力した場合は、スイッチ３１ｅ，３１ｆが２の状態に設定され、フィルタ係数の計算が行なわれる。このとき、加算器３１ｄの出力がスイッチ３１ｅ，３１ｆを介して減算器３１ｇ、３１ｈに入力され、あらかじめ具備されているパイロットシンボル３１ｉとの誤差が計算される。誤差は、係数生成部３１ｃに供給される。係数生成部３１ｃは、その誤差が最小となるような最適な係数C_1～C_Mを計算する。また、その係数C_1～C_Mが秘密鍵生成のために出力される。この生成器の構成は、図１１、図１２および図１３に示した構成に対応する。

【００７５】図３２は、この発明による秘密鍵生成器を搭載した無線通信システムで使用するパケットの第１の構成例を示す。端末局から基地局に伝送される上りパケット３２a_1，３２a_2，・・・と基地局から端末局に伝送される下りパケット３２ｂ１，３２ｂ２，・・・が同一のキャリア周波数で交互に伝送される。上りパケットおよび下りパケットの両パケットのデータ構成について説明する。

【００７６】１パケットは、パイロットシンボル３２ｃ、誤り検出を行なうＣＲＣ(CyclicRedundancy Check)符号によるパリティビット３２ｄ、暗号化された情報データ３２ｅから構成される。情報データは、情報シンボル３２f_1，３２f_2，・・・３２f_nから構成されている。ＣＲＣは、受信時にパリティビットチェックを行ない、誤りが検出された場合には、送信側に対して再送要求が行なわれる。なお、上りと下りパケットとは、基本的には同じ構成である。

【００７７】図３３は、この発明による秘密鍵生成器を搭載した無線通信システムで使用するパケットの第２の構成例を示す。当然のことながら基地局と端末局で生成した秘密鍵は本来、一致していなければならない。しかしながら、雑音または高速に移動する移動通信の伝搬環境下において伝搬路の状態が激変することによって両者で推定した伝搬路特性に差異が生じて生成した秘密鍵が異なる可能性がある。本構成は、基地局と端末局で生成した秘密鍵が異なった場合、それを検出・再生成させるための機能を付加したものである。

【００７８】端末局から基地局に伝送される上りパケット３３a_1，３３a_2，・・・と基地局から端末局に伝送される下りパケット３３b_1，３３b_2，・・・が同一のキャリア周波数で交互に伝送される。上りおよび下り両パケットの内部構成について説明する。パイロットシンボル３３ｃ、誤り検出を行なうＣＲＣ符号によるパリティビットＣＲＣ１３３ｄ、暗号化された情報データ３３ｅから構成される。情報データはパリティビットＣＲＣ２３３ｆ、情報シンボル３３g_1，３３g_2，・・・３３g_nから構成されている。

【００７９】ＣＲＣ１は、受信時にパリティチェックを行ない、ビット誤りが検出された場合には再送要求が行われる。ＣＲＣ２の機能について説明する。この発明によれば秘密鍵が基地局と端末局でそれぞれ生成されるが、伝搬環境によってはその秘密鍵は一致しない場合が有り得る。

【００８０】そこで、図３４に示すように、送信側では、例えば、基地局において、まず、ステップＳ１において、平文（元の情報データ）にパリティＣＲＣ２を付加する。ステップＳ２において、ＣＲＣ２を付加したデータに対して、基地局で生成した秘密鍵ｋＢを用いて暗号化を行なう。ステップＳ３において、パリティＣＲＣ１を付加した後に、ステップＳ４において変調し、端末局に送信する。

【００８１】受信側では図３５に示すように、端末局側では先ず、ステップＳ１１において、通常のＣＲＣ１による検査を行なう。ステップＳ１２では、検査の結果が合格か否かがチェックされる。合格が確認されれば、ステップＳ１４において、端末局で生成した秘密鍵ｋＴで暗号復号化を行なう。ＣＲＣ１による検査が不合格の場合では、ステップＳ１３において再送要求が行われる。

【００８２】ステップＳ１５では、復号化されたデータに対してＣＲＣ２を用いて検査を行なう。ステップＳ１６では、検査の結果が合格か否かがチェックされる。合格が確認されれば、ステップＳ１８において、復調されたデータが情報データとして出力される。

【００８３】両局の秘密鍵が異なっていれば、復号されたデータは正しいデータではなくビット誤りが発生するので、ステップＳ１６においてなされるＣＲＣ２による検査が不合格となる確率が高い。このときは、ステップＳ１７において、両局に対して秘密鍵の再生成・再暗号化・再送処理を要求する。それによって、両局の秘密鍵が異なっていることを検出できる。

【００８４】図３６は、この発明による秘密鍵生成器を搭載した無線通信システムで使用するパケットの第３の構成例を示す。基地局と端末局の両局で生成した秘密鍵が一致しない一つの原因として、生成した時刻間の時間差によって伝搬路が変化して両者で推定した遅延プロファイルまたは周波数特性が異なってしまうことが挙げら

れる。そこで、その時間差を極力小さくする必要がある。

【００８５】そこで、本パケット構成では、最初に、基地局が秘密鍵生成時に用いる上りパイロットシンボル３６ａを伝送し、その直後に直ちに端末局が秘密鍵生成時に用いる下りパイロットシンボル３６ｂを伝送する。その後に上りパケット$36c_1$，$36c_2$，・・・と下りパケット$36d_1$，$36d_2$・・・が交互に伝送される。これらのパケットの内部構造は、図３２または図３３で示した構造と同様である。

【００８６】図３７は、図３３，図３４，図３５，図３６に示した手法によってパケットを構成した場合の送受信処理のタイムチャートを示す。まず、処理ＳＴ１では、端末局から基地局に向けて上りパイロットシンボル３７ａを送信する。基地局では直ちに下りパイロットシンボル３７ｂを送信し、上りパイロットシンボルにより、伝搬路推定を行なって秘密鍵ｋＢ１を生成する（ＳＴ２）。一方、端末局においても下りパイロットシンボルにより伝搬路推定を行なって秘密鍵ｋＴ１を生成する（ＳＴ４）。

【００８７】そして、秘密鍵ｋＴ１を使用して情報データを暗号化して上りパケット３７ｃとして送信する（ＳＴ５）。処理ＳＴ６において、基地局ではこのパケットのＣＲＣ１に対する検査を行ない、合格したと仮定する。次に、秘密鍵ｋＢ１を使用して暗号復号化を行なった後にＣＲＣ２に対する検査を行ない、不合格であったと仮定する。ｋＢ１とＫＴ１は等しくないと判断する。そして、基地局が秘密鍵の再生成のために下りパイロットシンボル３７ｄを端末局に送信する（ＳＴ７）。

【００８８】端末局において受信後、このパイロットシンボル伝送を秘密鍵の再生成の要求と判断して、秘密鍵ｋＴ２を生成する（ＳＴ８）。直ちに上りパイロットシンボル３７ｅを送信する（ＳＴ９）。基地局においてパイロットシンボル受信後に秘密鍵ｋＢ２を生成する（ＳＴ１０）。秘密鍵ｋＢ２を用いて情報データを暗号化して下りパケット３７ｆとして送信する（ＳＴ１１）。

【００８９】端末局側では、処理ＳＴ１２において、ＣＲＣ１とＣＲＣ２に対する検査がともに合格したと仮定する。これによって秘密鍵ｋＴ２とｋＢ２が等しいと判断し、復号されたデータを情報データとみなす。次に、秘密鍵ｋＴ２を用いて情報データを暗号化して上りパケット３７ｇとして基地局に送信する（ＳＴ１３）。基地局では、秘密鍵ｋＢ２によって暗号復号化を行ない、復号されたデータを情報データとみなす（ＳＴ１４）。以下、同様にパケットの送受を行なって、通信を行なう。なお、パイロットシンボルの送受を頻繁に行って秘密鍵を生成・更新する頻度を高めれば信頼性をさらに向上させることが可能となる。

【００９０】この発明は、上述したこの発明の一実施形態等に限定されるものでは無く、この発明の要旨を逸脱しない範囲内で様々な変形や応用が可能である。例えば複素振幅情報、電力情報、位相情報の内の２以上の情報を使用して遅延プロファイルまたは周波数特性を推定するようにしても良い。また、図３２、図３３、または図３６にそれぞれ示すデータ構成は、情報データに限らず、ソフトウェア無線装置のプログラムデータの通信に対しても適用できる。また、上述した構成において、各構成要素をハードウエア以外にソフトウェアによって実現するようにしても良い。さらに、この発明は、陸上移動通信に限らず、固定通信に対しても同様に適用でき、さらに、屋内の無線ＬＡＮに対しても適用できる。

【００９１】

【発明の効果】以上のように、この発明によれば、情報データまたはソフトウェア無線通信機のプログラムを２局間に固有の伝搬路の状態を利用して秘密鍵番号を生成することによって、盗聴が困難な秘匿性の高い秘密鍵を生成することが可能となる。一般的に陸上移動体通信等で用いられる周波数が数ＧＨｚものマイクロ波やミリ波においては特定の２局間の伝搬路状態は基地局と他の端末局間の無線伝搬路の状態とは無相関であるからである。この発明は、秘密鍵を送信側と受信側とで共有するために、相手側に秘密鍵を伝送することがなく、セキュリティを高くすることができる。

【図面の簡単な説明】

【図１】従来の暗号化方式の一例を示すブロック図である。

【図２】従来の暗号化方式の他の例を示すブロック図である。

【図３】陸上移動通信における電波伝搬の様子を示す略線図である。

【図４】遅延プロファイルの例を示す略線図である。

【図５】遅延プロファイル測定のための送信装置の構成例を示すブロック図である。

【図６】遅延プロファイル測定のための受信装置の構成例を示すブロック図である。

【図７】伝搬路の複素遅延プロファイルの例を示す略線図である。

【図８】伝搬路の周波数特性の求める処理の一例を示すブロック図である。

【図９】伝搬路の周波数特性の求める処理の他の例を示すブロック図である。

【図１０】伝搬路の周波数特性の例を示す略線図である。

【図１１】電力情報による秘密鍵生成方法を説明するためのブロック図である。

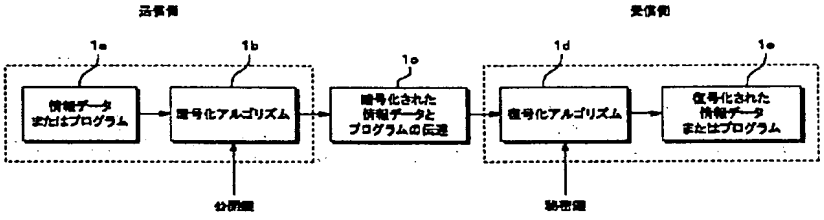
【図１２】振幅情報による秘密鍵生成方法を説明するためのブロック図である。

【図１３】位相情報による秘密鍵生成方法を説明するためのブロック図である。

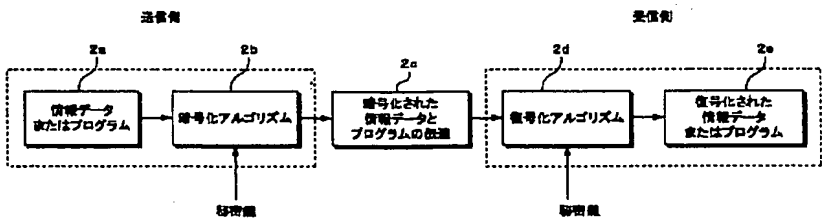
【図１４】Ｍ入力Ｎ出力選択器の構成例を示すブロック

図である。
【図１５】電力・秘密鍵生成器の構成例を示すブロック図である。
【図１６】電力計算回路の構成例を示すブロック図である。
【図１７】量子化回路の構成例を示すブロック図である。
【図１８】ビット結合器の構成例を示すブロック図である。
【図１９】振幅・秘密鍵生成器の構成例を示すブロック図である。
【図２０】位相・秘密鍵生成器の構成例を示すブロック図である。
【図２１】位相・ビット変換器のいくつかの動作例を示す略線図である。
【図２２】この発明をソフトウェア無線通信装置に適用した一実施形態のブロック図である。
【図２３】この発明の一実施形態における暗号化・ベースバンド変調部の構成例を示すブロック図である。
【図２４】この発明の一実施形態におけるＯＦＤＭ用ベースバンド復調・暗号化復号化・秘密鍵生成部の第１の構成例を示すブロック図である。
【図２５】この発明の一実施形態におけるＯＦＤＭ用ベースバンド復調・暗号化復号化・秘密鍵生成部の第２の構成例を示すブロック図である。
【図２６】この発明の一実施形態におけるスペクトラム拡散用方式用ベースバンド復調・暗号化復号化・秘密鍵生成部の第１の構成例を示すブロック図である。
【図２７】この発明の一実施形態におけるスペクトラム拡散用ベースバンド復調・暗号化復号化・秘密鍵生成部の第２の構成例を示すブロック図である。
【図２８】この発明の一実施形態におけるシングルキャリア方式用ベースバンド復調・暗号化復号化・秘密鍵生成部の第１の構成例を示すブロック図である。
【図２９】この発明の一実施形態におけるシングルキャリア方式用ベースバンド復調・暗号化復号化・秘密鍵生成部の第２の構成例を示すブロック図である。
【図３０】この発明の一実施形態におけるシングルキャリア方式用ベースバンド復調・暗号化復号化・秘密鍵生成部の第３の構成例を示すブロック図である。
【図３１】この発明の一実施形態におけるシングルキャリア復調器用等化器の構成例を示すブロック図である。
【図３２】この発明で使用できるパケットの構成の第１の例を示す略線図である。
【図３３】この発明で使用できるパケットの構成の第２の例を示す略線図である。
【図３４】第２のパケット構成を使用した場合の送信側の処理を説明するフローチャートである。
【図３５】第２のパケット構成を使用した場合の受信側の処理を説明するフローチャートである。
【図３６】この発明で使用できるパケットの構成の第３の例を示す略線図である。
【図３７】この発明が適用された無線通信システムにおけるパケット通信のタイミングチャートである。
【符号の説明】
３ａ・・・基地局、３ｂ・・・端末局、、２２ｊ・・・ベースバンド復調・暗号復号化・秘密鍵生成部、２２ｏ・・・プログラマブル復調部、２２ｐ・・・プログラマブル変調部、２２ｒ・・・暗号化・ベースバンド変調部、２２ｎ・・・変復調プログラムデータベース

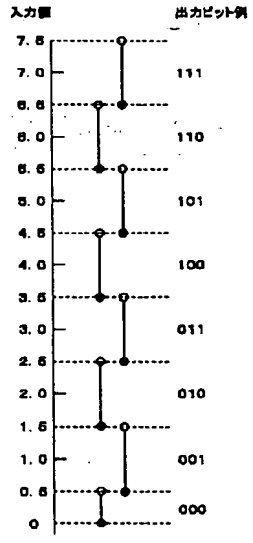
【図１】



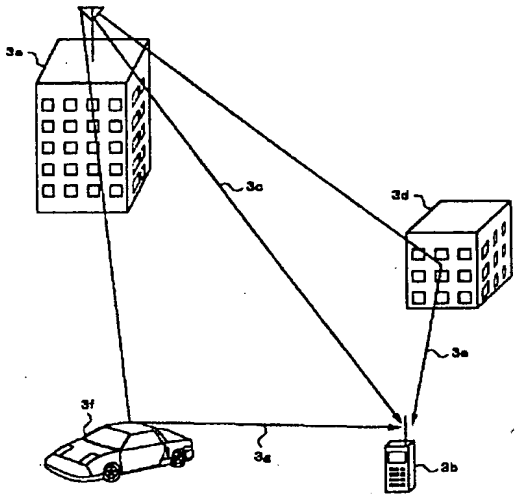
【図２】



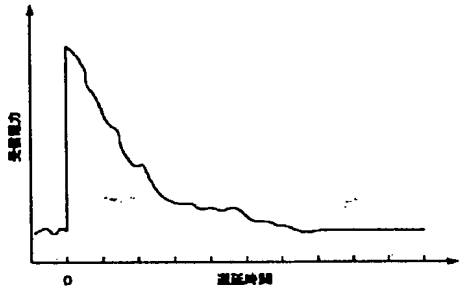
【図１７】



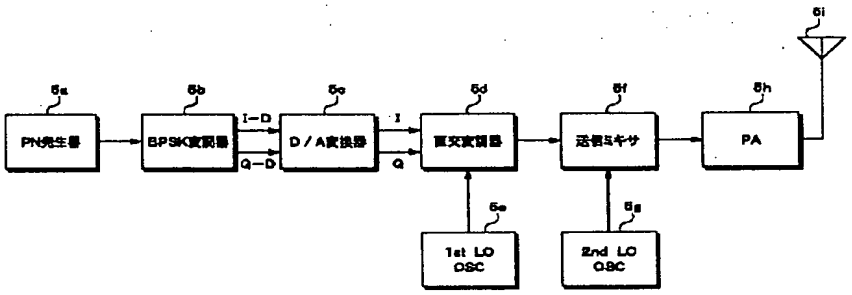
【図3】


3a
3c
3d
3e
3f
3g
3b

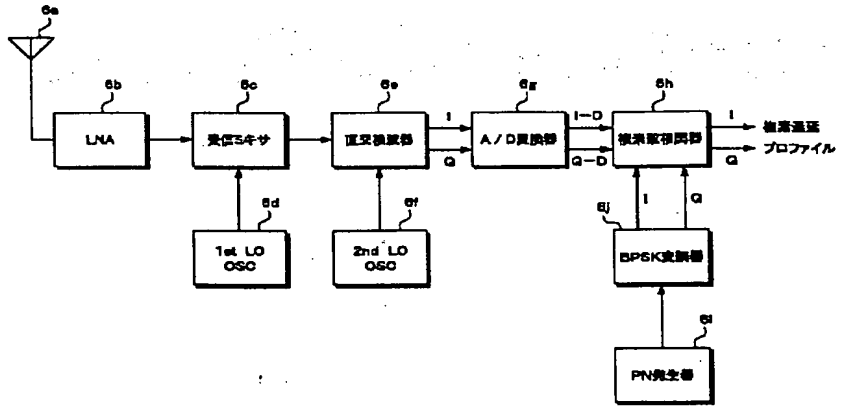
【図4】


受信電力
0
遅延時間

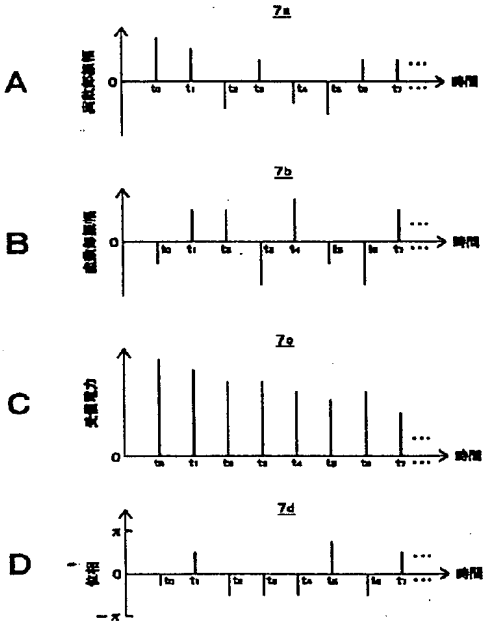
【図5】


5a
PN発生器
5b
BPSK変調器
I−D
Q−D
5c
D/A変換器
I
Q
5d
直交変調器
5e
1st LO OSC
5f
送信スキサ
5g
2nd LO OSC
5h
PA
5i

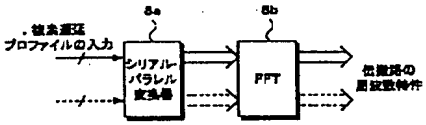
【図6】


6a
6b
LNA
6c
受信スキサ
6d
1st LO OSC
6e
直交検波器
I
Q
6f
2nd LO OSC
6g
A/D変換器
I−D
Q−D
6h
検索取得回路
I
Q
相関値
プロファイル
6i
PN発生器
6j
BPSK変調器
I
Q

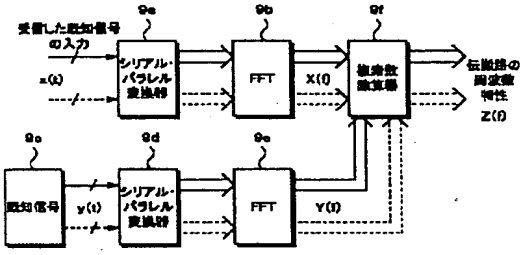
【図７】



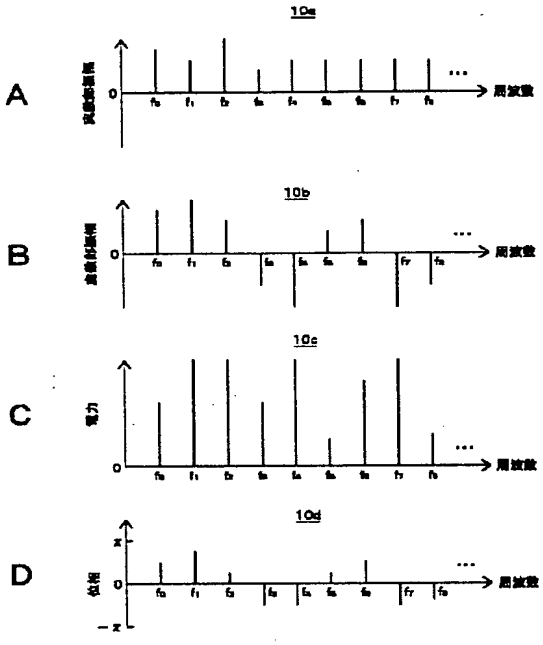
【図８】



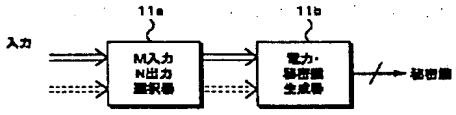
【図９】



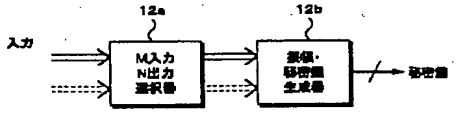
【図１０】



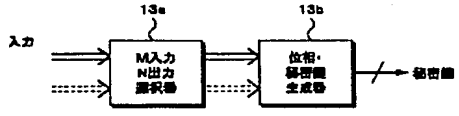
【図１１】



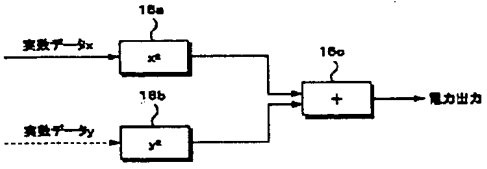
【図１２】



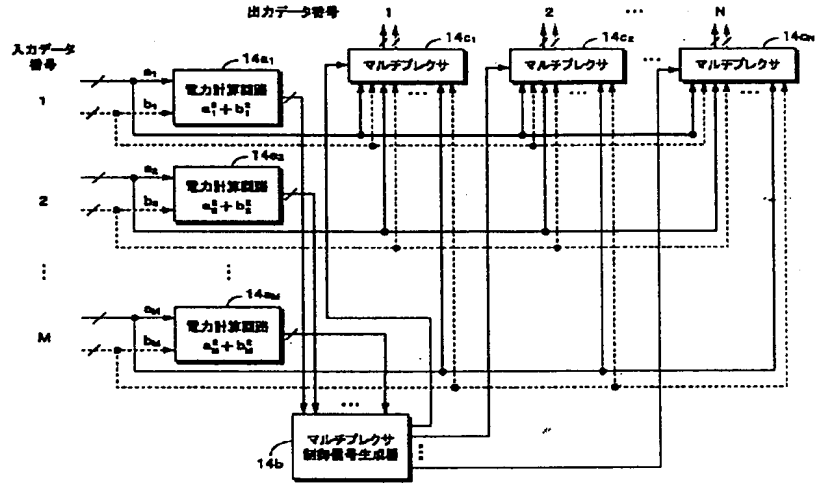
【図１３】



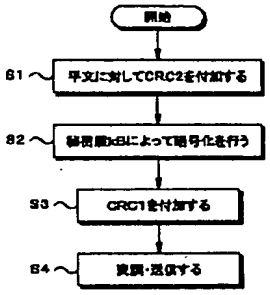
【図１６】



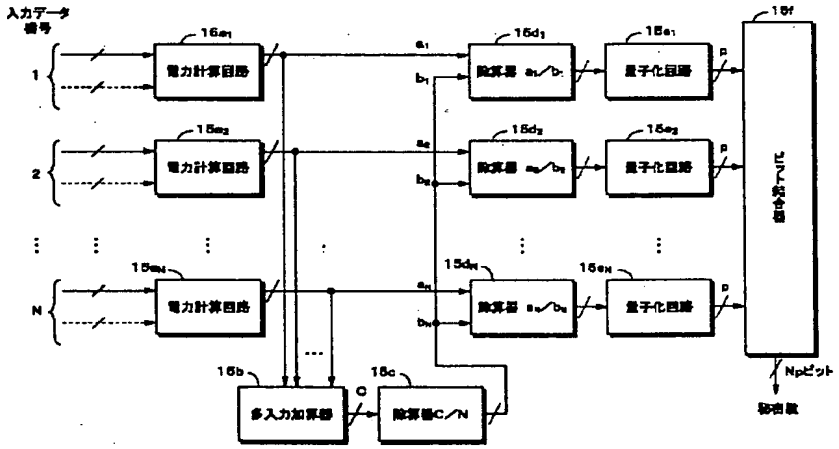
【図１４】



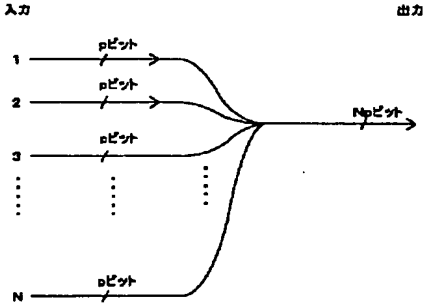
【図３４】



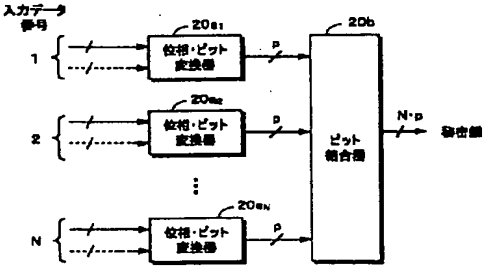
【図１５】



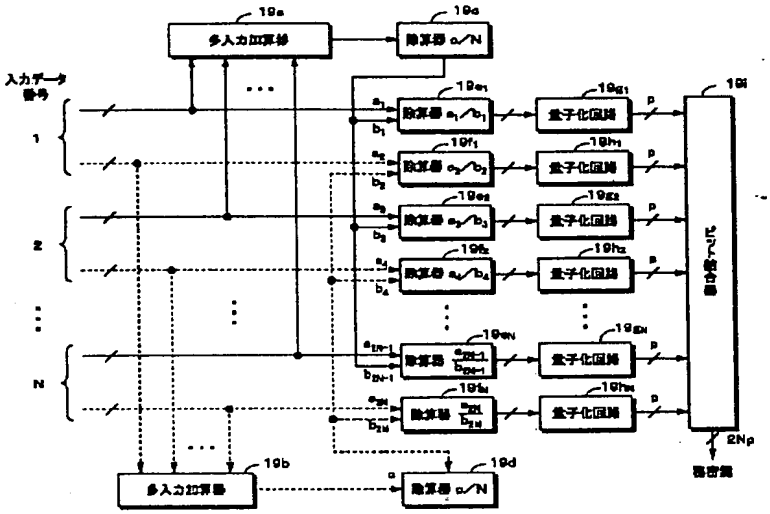
【図１８】



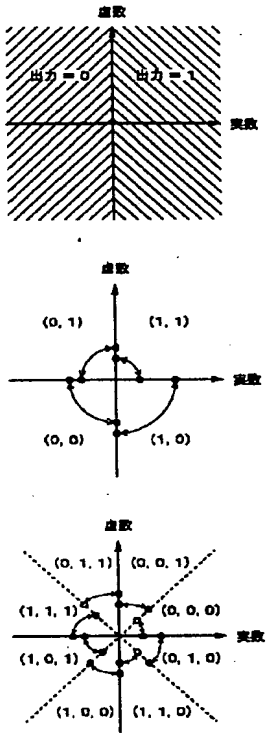
【図２０】



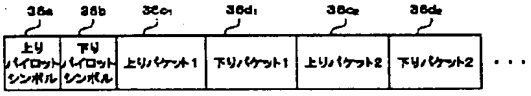
【図１９】



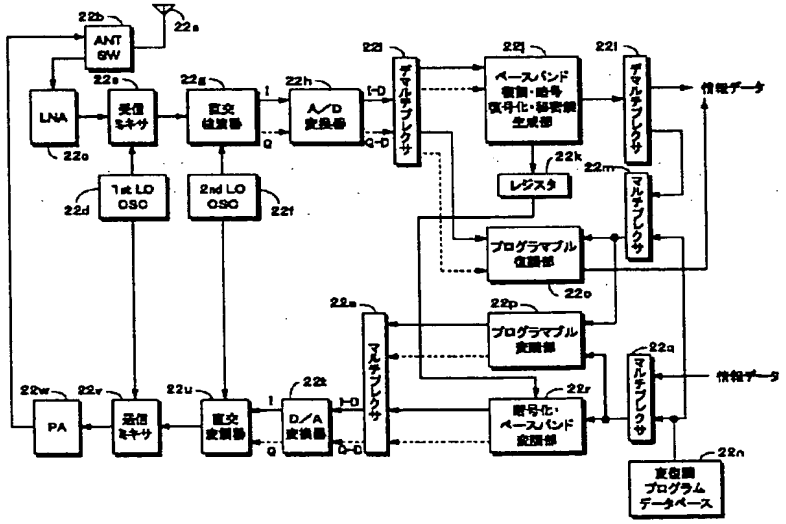
【図２１】



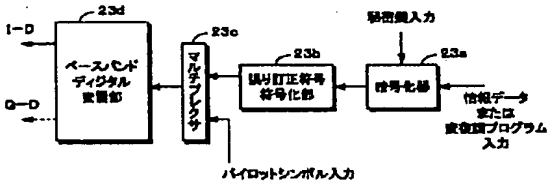
【図３６】



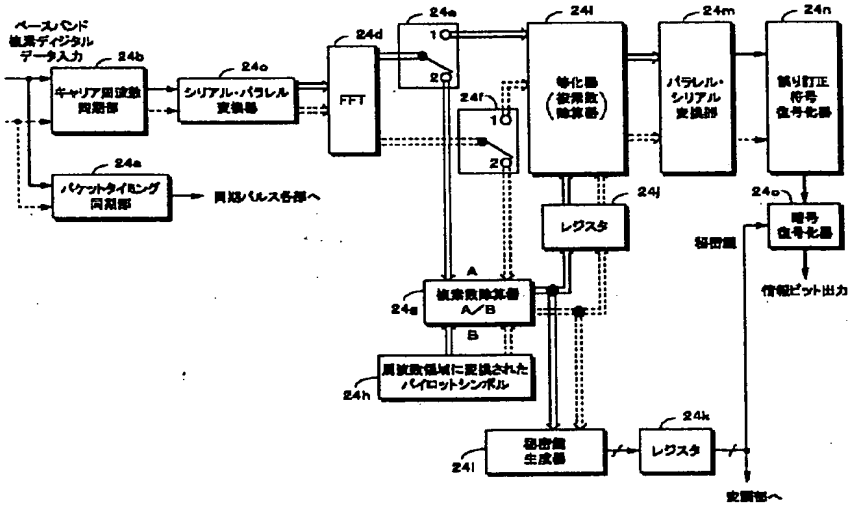
【図２２】



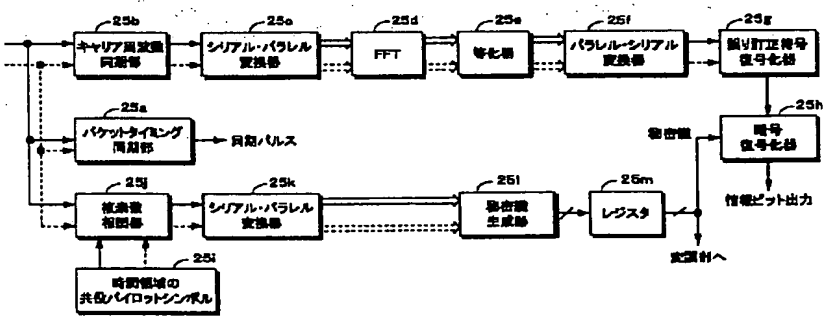
【図23】


I-D
Q-D
23d
ベースバンド
ディジタル
変調部
23c
マルチプレクサ
23b
誤り訂正符号
符号化部
23a
暗号化器
秘密鍵入力
情報データ
または
変復調プログラム
入力
パイロットシンボル入力

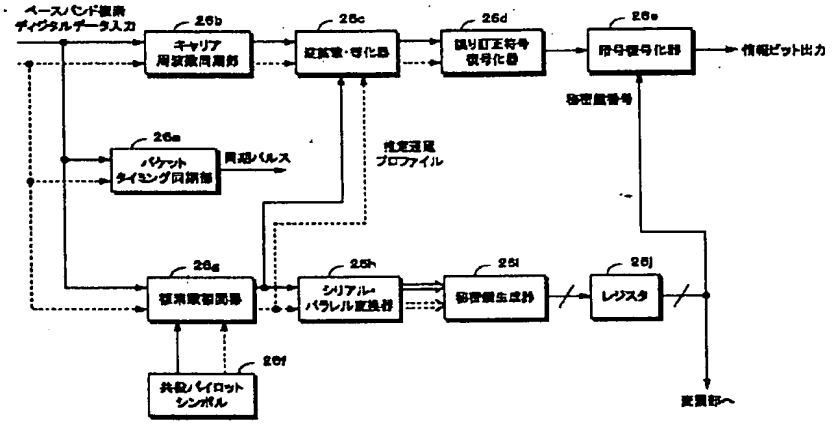
【図24】


ベースバンド
復調ディジタル
データ入力
24b
キャリア周波数
同期部
24c
シリアル・パラレル
変換器
FFT
24d
24e
1
2
24f
1
2
24i
等化器
(複素数
除算器)
24m
パラレル・
シリアル
変換部
24n
誤り訂正
符号
復号化器
24a
パケットタイミング
同期部
同期パルス各部へ
24j
レジスタ
24o
暗号
復号化器
秘密鍵
情報ビット出力
A
24g
複素数除算器
A/B
B
24h
周波数領域に変換された
パイロットシンボル
24k
秘密鍵
生成器
レジスタ
24l
変調部へ

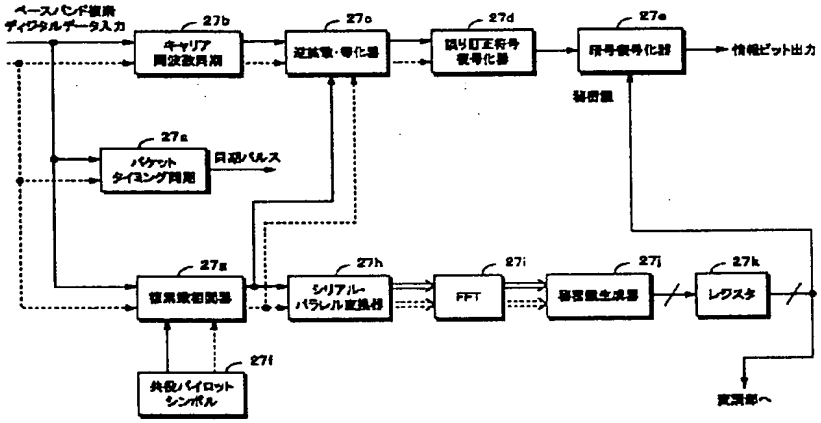
【図25】


25b
キャリア周波数
同期部
25c
シリアル・パラレル
変換器
25d
FFT
25e
等化器
25f
パラレル・シリアル
変換器
25g
誤り訂正符号
復号化器
25a
パケットタイミング
同期部
同期パルス
25h
暗号
復号化器
秘密鍵
情報ビット出力
25j
複素数
相関器
25k
シリアル・パラレル
変換器
25l
秘密鍵
生成部
25m
レジスタ
変調部へ
25i
時間領域の
共役パイロットシンボル

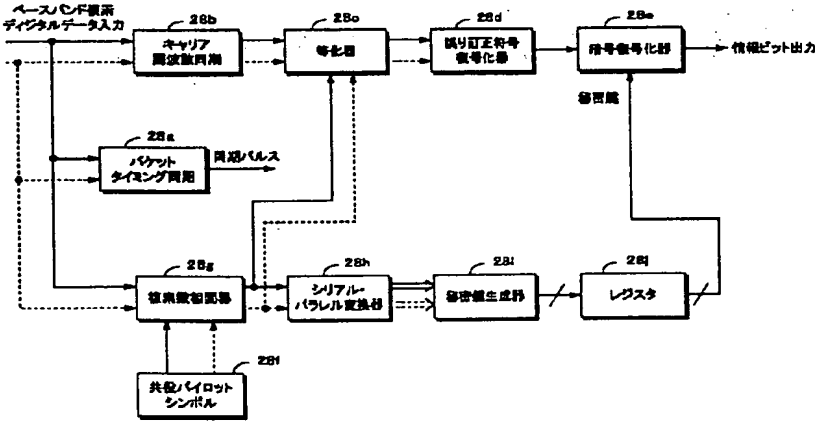
【図26】


ベースバンド復調ディジタルデータ入力
キャリア周波数同期部
逆拡散・等化器
誤り訂正符号復号化器
符号復号化部
情報ビット出力
秘密鍵情号
パケットタイミング同期部
同期パルス
推定遅延プロファイル
複素数相関器
シリアル・パラレル変換器
秘密鍵生成部
レジスタ
共役パイロットシンボル
変調部へ

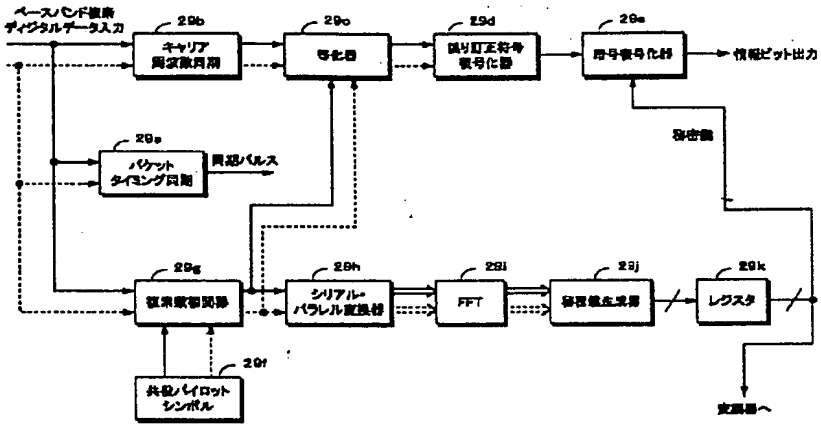
【図27】


ベースバンド復調ディジタルデータ入力
キャリア周波数同期
逆拡散・等化器
誤り訂正符号復号化器
符号復号化部
情報ビット出力
秘密鍵
パケットタイミング同期
同期パルス
複素数相関器
シリアル・パラレル変換器
FFT
秘密鍵生成器
レジスタ
共役パイロットシンボル
変調部へ

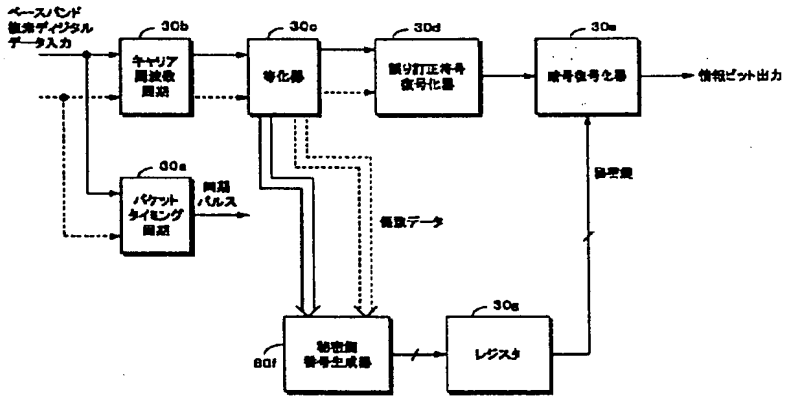
【図28】


ベースバンド復調ディジタルデータ入力
キャリア周波数同期
等化器
誤り訂正符号復号化器
符号復号化部
情報ビット出力
秘密鍵
パケットタイミング同期
同期パルス
複素数相関器
シリアル・パラレル変換器
秘密鍵生成部
レジスタ
共役パイロットシンボル

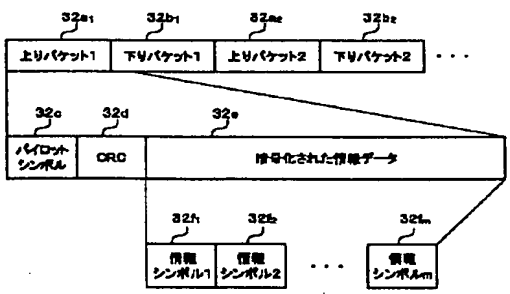
【図29】



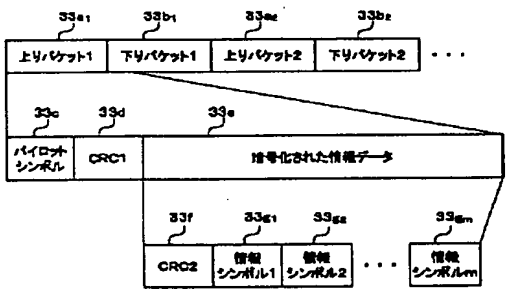
【図30】



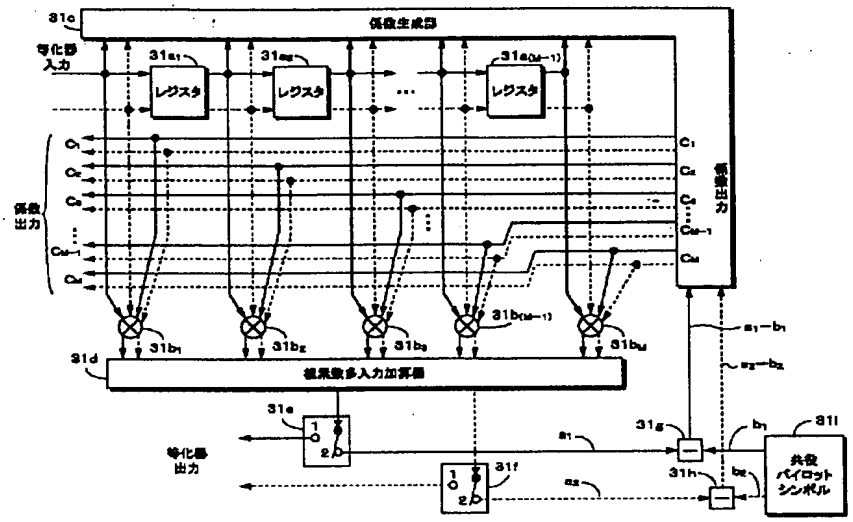
【図32】



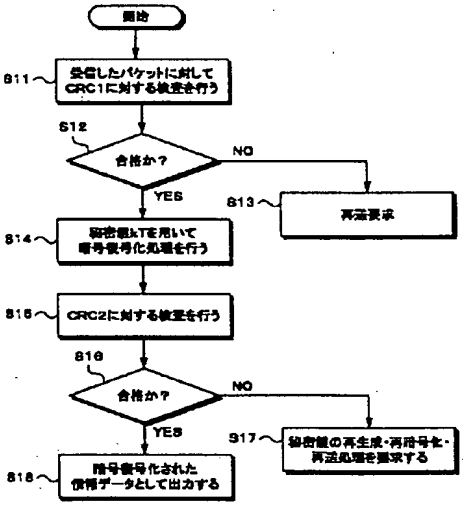
【図33】



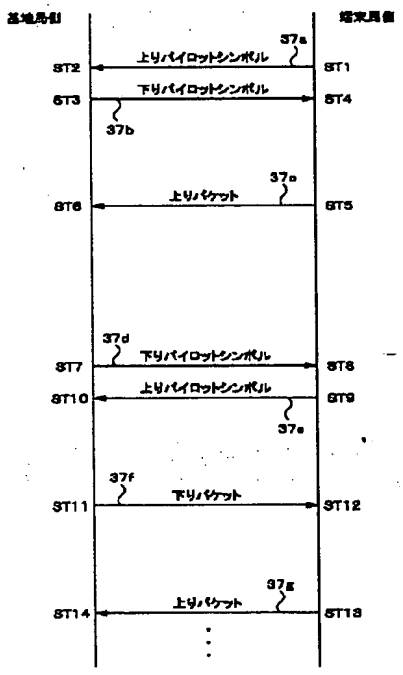
【図31】


係数生成器
等化器入力
レクスタ
係数出力
線形複多入力加算器
等化器出力
共役パイロットシンボル

【図35】


開始
受信したパケットに対してCRC1に対する検査を行う
合格か？
NO
YES
再送要求
秘密鍵kTを用いて暗号復号化処理を行う
CRC2に対する検査を行う
合格か？
NO
YES
秘密鍵の再生成・再暗号化・再送処理を要求する
暗号復号化された情報データとして出力する

【図37】


基地局側
端末局側
上りパイロットシンボル
下りパイロットシンボル
上りパケット
下りパケット
上りパケット
下りパイロットシンボル
上りパイロットシンボル
下りパケット
上りパケット

フロントページの続き

(51)Int.Cl.[7]	識別記号	FI	テーマコード(参考)
		H04J 13/00	A

(72)発明者 原田 博司
東京都小金井市貫井北町4−2−1 独立行政法人通信総合研究所内
(72)発明者 藤瀬 雅行
東京都小金井市貫井北町4−2−1 独立行政法人通信総合研究所内

Fターム(参考) 5J104 AA16 EA04 EA24 JA03 NA02 PA01
5K022 DD01 DD13 DD19 DD23 DD33 EE02 EE14 EE22 EE32
5K067 AA30 AA33 BB04 BB21 CC04 DD17 HH36